POINT Guard I/O-Sicherheitsmodule

Allen-Bradley

Bestellnummern 1734-IB8S, 1734-OB8S

Installations- und Benutzerhandbuch

Allen-Bradley • Rockwell Software

Rockwell Automation

Wichtige Hinweise für den Anwender

Die Betriebseigenschaften elektronischer Geräte unterscheiden sich von denen elektromechanischer Geräte. In der Publikation SGI-1.1 „Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls“ (erhältlich bei Ihrem Rockwell Automation-Vertriebsbüro oder online unter http://www.rockwellautomation.com/literature/) werden einige wichtige Unterschiede zwischen elektronischen und festverdrahteten elektromechanischen Geräten beschrieben. Aufgrund dieser Unterschiede und der vielfältigen Einsatzbereiche elektronischer Geräte müssen die für die Anwendung dieser Geräte verantwortlichen Personen sicherstellen, dass die Geräte zweckgemäß eingesetzt werden.

Rockwell Automation ist in keinem Fall verantwortlich oder haftbar für indirekte Schäden oder Folgeschäden, die durch den Einsatz oder die Anwendung dieses Geräts entstehen.

Die in diesem Handbuch aufgeführten Beispiele und Abbildungen dienen ausschließlich der Veranschaulichung. Aufgrund der unterschiedlichen Anforderungen der jeweiligen Anwendung kann Rockwell Automation keine Verantwortung oder Haftung für den tatsächlichen Einsatz der Produkte auf der Grundlage dieser Beispiele und Abbildungen übernehmen.

Rockwell Automation übernimmt keine patentrechtliche Haftung in Bezug auf die Verwendung von Informationen, Schaltkreisen, Geräten oder Software, die in dieser Publikation beschrieben werden.

Die Reproduktion dieser Bedienungsanleitung ist – ob vollständig oder in Teilen – verboten, sofern keine schriftliche Genehmigung von Rockwell Automation, Inc., vorliegt.

In dieser Publikation werden folgende Hinweise verwendet, um Sie auf bestimmte Sicherheitsaspekte aufmerksam zu machen.

WARNUNG	Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die in explosionsgefährdeten Umgebungen zu einer Explosion und damit zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können.
WICHTIG	Dieser Hinweis enthält Informationen, die für den erfolgreichen Einsatz und das Verstehen des Produkts besonders wichtig sind.
ACHTUNG	Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können. Die Achtungshinweise helfen Ihnen, eine Gefahr zu erkennen, die Gefahr zu vermeiden und die Folgen abzuschätzen.
STROMSCHLAG-GEFAHR	An der Außenseite oder im Inneren des Geräts (z. B. des Antriebs oder Motors) kann ein Etikett dieser Art angebracht sein, das Sie darauf hinweist, dass eine gefährliche Spannung anliegen kann.
VERBRENNUNGS-GEFAHR	An der Außenseite oder im Inneren des Geräts (z. B. des Antriebs oder Motors) kann ein Etikett dieser Art angebracht sein, das Sie darauf hinweist, dass die Oberflächen gefährliche Temperaturen erreichen können.

Allen-Bradley, Rockwell Automation, POINT Guard I/O, POINTBus, POINT I/O, RSLogix 5000, RSLinx, RSNetWorx for DeviceNet, SmartGuard, GuardPLC, ControlLogix, GuardLogix, GuardShield, CompactBlock Guard I/O und TechConnect sind Marken von Rockwell Automation.

Nicht Rockwell Automation gehörende Marken sind Eigentum der jeweiligen Rechtsinhaber.

Diese Publikation enthält neue und überarbeitete Informationen, die in der letzten Version nicht enthalten waren.

Überarbeitete Informationen

Die Tabelle enthält eine Zusammenfassung der wichtigsten Änderungen an diesem Handbuch.

Überarbeitung zum Thema	Siehe
Internationale ISO-Norm	36
Europäische IEC-Norm	36
Umgebung und Gehäuse	44
Ziehen und Stecken unter Spannung	48
Überwachen der Attribut-ID für einen Testausgangsstatus	148
Internationale ISO-Norm	149
1734-IB8S-Spannungsbereich	155
Spezifikation der Eingangsspannung im Aus-Zustand	155
1734-IB8S-Temperaturbereich	156
1734-OB8S-Temperaturbereich	157
Spezifikation der Isolationsspannung	158
Temperaturcode Nordamerika	158
Betriebstemperaturbereich	159
Spezifikation der Störfestigkeit bei abgestrahlten Hochfrequenzstörungen	159
CE-Zertifizierung	160
TÜV-Zertifizierung	160

Neue Informationen

Die Tabelle enthält eine Zusammenfassung der wichtigsten Neuerungen in diesem Handbuch.

Neue Informationen zu folgendem Thema	Siehe
Europäische Zulassung für explosionsgefährdete Standorte	37
Warnhinweis zur europäischen Zertifizierung für Zone 2	37
Nordamerikanische Zulassung für explosionsgefährdete Standorte	40
Festlegen der Netzknotenadresse eines POINT Guard I/O-Moduls	52
Zurücksetzen der POINT Guard I/O-Module auf die Werkseinstellungen	55
Automatische Adressierung mit einem 1734-PDN-Adapter und mit POINT Guard I/O-Modulen	56
IEC-Temperaturcode	158

Neue Informationen zu folgendem Thema	Siehe
c-UL-us-Zertifizierung	160
Ex-Zertifizierung	160
ODVA-Zertifizierung	160

Änderungsbalken

Änderungsbalken (wie in diesem Abschnitt dargestellt) zeigen, welche Abschnitte in diesem Handbuch sich von den vorherigen Ausgaben unterscheiden. Sie weisen außerdem auf neue oder überarbeitete Informationen hin.

Vorwort

Verwendung dieses Handbuchs 9
Konventionen in diesem Handbuch 9
Informationen zu den technischen Daten und Abmessungen in diesem Handbuch 9
Terminologie 9

Kapitel 1

POINT Guard I/O – Überblick

Einleitung 13
Vorbereitungen 14
Informationen zur Einsatzeignung 14
Zu beachtende Vorsichtsmaßnahmen für die Verwendung . . 15
Vorsichtsmaßnahmen für Montage, Verdrahtung und Reinigung 17
E/A-Module – Überblick 17
Architektur des Sicherheitssystems 19
CIP Safety-Architekturen 20
Anforderungen an Sicherheitsanwendungen 21
- Sicherheitsnetzwerknummer 21
- Sicherheitssignatur 21

Kapitel 2

Sicherheitsfunktionen

Einleitung 23
E/A-Sicherheitsmodule 23
Sicherheitseingänge 24
- Verwenden eines Testausgangs mit einem Sicherheitseingang 24
- Einzelkanalmodus 26
- Zweikanalmodus und Diskrepanzzeit 27
- Zwei Kanäle, gleichwertig 28
- Zwei Kanäle, komplementär 29
- Wiederherstellung nach einem Fehler des Sicherheitseingangs 31
- Eingangsverzögerungen 31

Sicherheitsausgänge 32
- Sicherheitsausgang mit Testimpuls 32
- Zweikanalige Einstellung 33
- Wiederherstellung nach einem Fehler des Sicherheitsausgangs 33

E/A-Statusdaten 34
Anforderungen für Steuergeräte 35
Sicherheitsmaßnahmen 36
Gesetzgebung und Industrienormen 36
- Europa 37
- EU-Richtlinien 38
- EMV-Richtlinie 38
- Nordamerika 39

Japan 41

Kapitel 3

Installation des Moduls

Einleitung 43
Umgebung und Gehäuse 44
Verhinderung elektrostatischer Entladung 45
Installieren des Montagesockels 46
Anschließen des Moduls am Montagesockel 48
Anschließen der abnehmbaren Klemmenleiste 49
Ausbauen eines Montagesockels 50
Verdrahten der Module 50
Festlegen der Netzknotenadresse eines POINT Guard I/O-Moduls 52
Zurücksetzen der POINT Guard I/O-Module auf die Werkseinstellungen 55
Automatische Adressierung mit einem 1734-PDN-Adapter und mit POINT Guard I/O-Modulen 56

Kapitel 4

Verdrahtung des Moduls

Einleitung 59
Verbindungsdetails 59
Beispiele für Verdrahtungen 61
Zweikanalige Not-Halt-Geräte 61
Zweikanalige Sicherheitsschütze 64

Kapitel 5

Beispiele für Netzteile

Einleitung 67
POINTBus-Backplane 67
Beispiele für Netzteile 68
Beispiel 1: POINT Guard I/O mit 1734-EP24DC (Eingang), 1734-FPD (Ausgang) – Nur 24-V-DC-E/A 69
Beispiel 2: POINT Guard I/O mit 1734-EP24DC für Eingang und Ausgang, plus AC-E/A 70
Vorsichtsmaßnahmen für die sichere Verwendung 71

Kapitel 6

Konfiguration des Moduls in einer GuardLogix-Steuerung

Einleitung 73
Verwenden der Hilfe 74
Hinzufügen von Modulen zum E/A-Konfigurationsbaum 74
Hinzufügen und Konfigurieren des Ethernet-Bridge-Moduls 74
Hinzufügen und Konfigurieren des 1734-AENT-Adapters 78
Hinzufügen und Konfigurieren von Sicherheitseingangsmodulen 82

Hinzufügen und Konfigurieren von Sicherheitsausgangsmodulen 88
Werte und Zustände von Tags 93
Konfigurieren der Registerkarte „Safety“ (Sicherheit) 94
Verwaltungsrechte für die Konfiguration 97
Konfigurationssignatur 97
Konfigurieren der Registerkarte „Input Configuration“ (Eingangskonfiguration) 98
Konfigurieren der Registerkarte „Test Output“ (Testausgang) 102
Konfigurieren der Registerkarte „Output Configuration“ (Ausgangskonfiguration) 103
Speichern und Herunterladen der Modulkonfiguration 105

Kapitel 7

Konfiguration des Moduls für eine SmartGuard-Steuerung

Einleitung 107
Vorbereitungen 107
Verwenden der Hilfe 108
Arbeiten mit der Software RSNetWorx for DeviceNet 108
Einrichten der Sicherheitskonfiguration 110
Arbeiten mit Eingängen 110
Arbeiten mit Ausgängen 114
Konfigurieren Sie die Eingangs- und Ausgangsverbindungen der SmartGuard-Steuerung 116
Abschließen der Konfiguration der SmartGuard-Steuerung 120
Speichern und Herunterladen der Modulkonfiguration 121

Kapitel 8

Überlegungen beim Ersetzen der POINT Guard I/O-Module

Inhalt dieses Kapitels 123
Überlegungen beim Ersetzen der POINT Guard I/O-Module 123
Warum die SNN manuell festgelegt werden muss 125
GuardLogix-Steuerungen im Vergleich zu SmartGuard-Steuerungen 126
Ersetzen eines E/A-Moduls, wenn eine SmartGuard-Steuerung verwendet wird 126
Ersetzen eines E/A-Moduls, wenn eine GuardLogix-Steuerung verwendet wird 130
E/A-Austausch mit aktivierter Option „Configure Only When No Safety Signature Exists“ (Nur konfigurieren, wenn keine Sicherheitssignatur vorhanden ist) 130
E/A-Austausch mit aktivierter Option „Configure Always“ (Immer konfigurieren) 137

Kapitel 9

Statusanzeigen
Einleitung . . . 141
Modulstatus . . . 142
Netzwerkstatus . . . 142
Konfigurationssperre . . . 143
Spannungsversorgung . . . 143
Status des sicheren Eingangs (1734-IB8S-Modul) . . . 143
Status des sicheren Ausgangs (1734-OB8S-Modul) . . . 144

Anhang A

Abrufen des E/A-Diagnosestatus von Modulen in Logix-Systemen
Einleitung . . . 145
Nachrichtenbefehle . . . 145
Konfigurieren Sie den Nachrichtenbefehl . . . 146

Anhang B

Versagenswahrscheinlichkeit bei Anforderung (PFD), Versagenswahrscheinlichkeit pro Stunde (PFH) und mittlerer Ausfallabstand (MTBF)
Inhalt dieses Anhangs . . . 149
Berechnete Werte . . . 149

Anhang C

Referenzinformationen zur Konfiguration
Inhalt dieses Anhangs . . . 151
Informationen zu den Parametergruppen . . . 151

Anhang D

Spezifikationen
Einleitung . . . 155

Anhang E

E/A-Baugruppen
Einleitung . . . 161
Eingangsbaugruppen . . . 161
Ausgangsbaugruppen . . . 163
Konfigurationsbaugruppen . . . 164

Anhang F

Weitere Informationen
Zugehörige Dokumentation . . . 167

Index

Verwendung dieses Handbuchs

Bevor Sie die POINT Guard I/O-Module verwenden, sollten Sie dieses Handbuch gelesen und verstanden haben. Falls Sie Fragen oder Anregungen haben, wenden Sie sich an Ihren Rockwell Automation-Vertreter.

Konventionen in diesem Handbuch

Diese Konventionen werden im gesamten Handbuch verwendet:

- Nummerierte Listen enthalten aufeinander folgende Schritte.
- Listen mit Aufzählungszeichen enthalten Informationen, keine aufeinander folgenden Schritte.

Informationen zu den technischen Daten und Abmessungen in diesem Handbuch

Änderungen der technischen Daten und Zubehörteile der Produkte bleiben zum Zwecke von Verbesserungen oder aus anderen Gründen vorbehalten. Bei Rückfragen zu den tatsächlichen technischen Daten eines erworbenen Produkts wenden Sie sich an Ihren Rockwell Automation-Vertreter. Abmessungen und Gewichte sind Nennwerte und eignen sich nicht für Fertigungszwecke, auch wenn Toleranzwerte angegeben sind.

Terminologie

Informationen zur Bedeutung häufig verwendeter Begriffe finden Sie in dieser Tabelle.

Begriff	Bedeutung
Verbindung	Logischer Kommunikationskanal für die Kommunikation zwischen Netzknoten. Die Verbindungen werden zwischen Mastern und Slaves verwaltet und gesteuert.
EDS	Akronym für „Electronic Data Sheet" (elektronisches Datenblatt). Eine Vorlage, die von der Software RSNetWorx verwendet wird, um die Konfigurationsparameter, das E/A-Datenprofil und die Verbindungsunterstützung für ein bestimmtes E/A-Modul anzuzeigen. Die RSNetWorx-Software verwendet diese einfachen Textdateien, um Produkte zu erkennen und diese in einem Netzwerk in Betrieb zu nehmen.
MTBF	Akronym für „Mean Time Between Failure" (mittlerer Ausfallabstand), also die durchschnittliche Zeit zwischen dem Auftreten von Ausfällen.
ODVA	Akronym für „Open DeviceNet Vendor Association" (offene Vereinigung für DeviceNet-Anbieter). Hierbei handelt es sich um eine gemeinnützige Vereinigung von Herstellern, die zur Förderung von CIP-Netzwerken gegründet wurde.
PFD	Akronym für „Probability of Failure on Demand" (Versagenswahrscheinlichkeit bei Anforderung), also mit welcher Wahrscheinlichkeit ein System im Schnitt seine vorgesehene Funktion bei Anforderung nicht ausführt.
PFH	Akronym für „Probability of Failure per Hour" (Versagenswahrscheinlichkeit pro Stunde), also mit welcher Wahrscheinlichkeit bei einem System pro Stunde ein gefährlicher Ausfall auftritt.

Begriff	Bedeutung
Bewährungs-prüfung	Regelmäßige Prüfung, die zum Erkennen von Fehlern in einem Sicherheitssystem ausgeführt wird, damit der ursprüngliche Zustand eines Systems oder ein diesem Zustand nahekommender Zustand bei Anforderung wiederhergestellt werden kann.
SNN	Akronym für „Safety Network Number" (Sicherheitsnetzwerknummer). Hierbei handelt es sich um eine Zahl, die ein Netzwerk unter allen Netzwerken in einem Sicherheitssystem eindeutig identifiziert. Sie sind dafür verantwortlich, jedem Sicherheitsnetzwerk oder Sicherheitsteilnetz innerhalb eines Systems eine eindeutige Nummer zuzuordnen.
Standard	Geräte oder Geräteteile, die nicht Teil der Sicherheitsfunktion sind.

Notizen:

POINT Guard I/O – Überblick

Thema	Seite
Einleitung	13
Vorbereitungen	14
Informationen zur Einsatzeignung	14
Zu beachtende Vorsichtsmaßnahmen für die Verwendung	15
Vorsichtsmaßnahmen für Montage, Verdrahtung und Reinigung	17
E/A-Module – Überblick	17
Architektur des Sicherheitssystems	19
CIP Safety-Architekturen	20
Anforderungen an Sicherheitsanwendungen	21

Einleitung

Verwenden Sie die POINT Guard I/O-Sicherheitsmodule in der POINT I/O-Plattform, um Sicherheits-E/A auf einem GuardLogix- oder SmartGuard-System zu verteilen. Sie können die Module mithilfe des Tools zur Netzwerkkonfiguration, der RSNetWorx-Software, des GuardLogix-Programmiertools oder der RSLogix 5000-Software, Version 17 oder höher, konfigurieren. GuardLogix-Systeme wurden für den Einsatz von POINT Guard I/O-Modulen mit einem EtherNet/IP-Adapter konzipiert.

Die Montagesockelbaugruppe (Bestellnummer 1734-TB oder 1734-TBS) besteht aus einem Montagesockel und einer abnehmbaren Klemmenleiste. Alternativ hierzu können Sie den einteiligen POINT I/O-Montagesockel verwenden (Bestellnummern 1734-TOP, 1734-TOPS, 1734-TOP3 oder 1734-TOP3S).

WICHTIG Sie benötigen für jedes 1734-IB8S- oder 1734-OB8S-Modul zwei Montagesockelbaugruppen. Verwenden Sie nicht die Montagesockelbaugruppen 1734-TB3 oder 1734-TB3S.

Vorbereitungen

Beachten Sie beim Verwenden eines Moduls stets die folgenden Richtlinien. Unter einem Sicherheitsadministrator wird in diesem Handbuch eine Person verstanden, die qualifiziert ist, über die erforderlichen Berechtigungen verfügt und dafür verantwortlich ist, die Sicherheit hinsichtlich Design, Installation, Betrieb, Wartung und Entsorgung der Maschine zu gewährleisten.

- Bevor Sie das Modul installieren und in Betrieb nehmen, sollten Sie dieses Handbuch gewissenhaft gelesen und verstanden haben. Lesen Sie bei Bedarf zusätzlich die entsprechende Dokumentation, die in Anhang F aufgeführt ist.
- Bewahren Sie das Handbuch an einem sicheren Ort auf, an dem die Mitarbeiter bei Bedarf darauf zugreifen können.
- Verwenden Sie das Modul ordnungsgemäß und abhängig von der Installationsumgebung, der Leistung und den Funktionen der Maschine.
- Stellen Sie sicher, dass ein Sicherheitsadministrator vor der Installation eine Risikobewertung an der Maschine vornimmt und die Eignung des Moduls bestimmt.

Vergewissern Sie sich vor der Inbetriebnahme des Sicherheitssystems, dass Sie die richtige POINT Guard I/O-Firmwareversion verwenden. Informationen zu den Firmwareversionen für die entsprechenden Sicherheitssteuerungen finden Sie unter http://www.rockwellautomation.com/products/certification/safety.

Informationen zur Einsatzeignung

Rockwell Automation ist nicht für die Konformität mit Normen, Vorschriften oder Bestimmungen verantwortlich, welche für die Kombination von Produkten innerhalb der Anwendung des Kunden oder für die Verwendung des Produkts gelten.

Ergreifen Sie alle erforderlichen Maßnahmen, um die Eignung des Produkts für die Systeme, Maschinen und Anlagen zu ermitteln, in denen es eingesetzt wird.

Beachten Sie alle für den Einsatz dieses Produkts geltenden Verbote und Einschränkungen.

Setzen Sie die Produkte nie in Bereichen ein, in denen es zu schwerwiegenden Personen- oder Sachschäden kommen kann, ohne zuvor sicherzustellen, dass das System insgesamt unter Berücksichtigung solcher Risiken entwickelt wurde. Zudem muss das Rockwell Automation-Produkt geeignete Nennwerte aufweisen und bestimmungsgemäß in der Ausrüstung bzw. Maschine installiert worden sein.

Zu beachtende Vorsichtsmaßnahmen für die Verwendung

ACHTUNG

Der Sicherheitszustand der Ausgänge ist als AUS-Zustand definiert. Ausführliche Informationen zum Sicherheitszustand der Eingänge finden Sie in Kapitel 2.

Der Sicherheitszustand des Moduls und seiner Daten ist als AUS-Zustand definiert.

Verwenden Sie das POINT Guard I/O-Modul ausschließlich in Anwendungen, in denen der AUS-Zustand der Sicherheitszustand ist.

Ein Durchschlag an den Sicherheitsausgängen kann zu ernsthaften Verletzungen führen. Schließen Sie keine die Nennwerte überschreitenden Lasten an die Sicherheitsausgänge an.

Ein Verlust der Sicherheitsfunktionen kann zu ernsthaften Verletzungen führen. Verdrahten Sie das Modul so, dass die Speise- oder Lastspannungen die Sicherheitsausgänge weder unbeabsichtigt noch versehentlich berühren.

ACHTUNG

Befolgen Sie diese Vorsichtsmaßnahmen, um eine sichere Verwendung zu gewährleisten:

Bevor Sie das System in Betrieb nehmen, müssen Sie die Leiter ordnungsgemäß verdrahten und sicherstellen, dass das Modul funktioniert. Eine falsche Verdrahtung kann zum Verlust der Sicherheitsfunktion führen.

Legen Sie keine Gleichstromspannungen an, die die Modulnennwerte überschreiten.

Legen Sie an den Moduleingängen die richtigen Spannungen an. Das Anlegen ungeeigneter Spannungen kann zu Fehlfunktionen des Moduls führen, also den Verlust von Sicherheitsfunktionen und Beschädigungen des Moduls mit sich bringen.

Verwenden Sie niemals Testausgänge als Sicherheitsausgänge. Testausgänge sind keine Sicherheitsausgänge.

Vergewissern Sie sich, dass nach der Installation des Moduls ein Sicherheitsadministrator die Installation bestätigt und einen Probelauf sowie eine Probewartung durchführt.

Das Modul darf nicht zerlegt, repariert oder modifiziert werden. Durch solche Maßnahmen kann es zum Verlust der Sicherheitsfunktionen kommen.

Verwenden Sie ausschließlich Komponenten und Geräte, die den einschlägigen Sicherheitsstandards für die erforderliche Sicherheitskategorie und Sicherheitsintegritätsstufe (SIL) entsprechen.

- Die Einhaltung der Anforderungen der jeweiligen Sicherheitskategorie und der Sicherheitsintegritätsstufe (SIL) muss für das gesamte System bestimmt werden.
- Wir empfehlen, die Einhaltung der erforderlichen Sicherheitsintegritätsstufe (SIL) oder Sicherheitskategorie durch eine Zertifizierungsgesellschaft bestätigen zu lassen.

Beachten Sie, dass der Anwender die Einhaltung der gültigen Industrienormen für das gesamte System bestätigen muss.

Trennen Sie das Modul von der Stromzufuhr, bevor Sie es verdrahten. Geräte, die am Modul angeschlossen sind, können unerwartet starten, wenn die Verdrahtung bei anliegender Spannung vorgenommen wird.

Vorsichtsmaßnahmen für Montage, Verdrahtung und Reinigung

Beachten Sie diese Vorsichtsmaßnahmen, um Betriebsausfälle, Fehlfunktionen oder unerwünschte Auswirkungen auf die Produktleistung zu vermeiden.

Befolgen Sie beim Stecken und Ziehen die Anweisungen für die Klemmeneinheit.

Gehen Sie beim Verdrahten der Module wie folgt vor:

- Verlegen Sie Kommunikations- und E/A-Leitungen niemals in einem Kabelkanal oder in einer Führungsschiene, wenn dort Hochspannungsleitungen verlegt sind.
- Nehmen Sie die Verdrahtung ordnungsgemäß und unter Beachtung der Signalnamen aller Klemmen vor.
- Befolgen Sie die in den Installationsanleitungen für die Klemmeneinheit angegebenen Drehmomentspezifikationen.

Verwenden Sie beim Reinigen von Modulen niemals folgende Stoffe:

- Verdünner
- Benzol
- Azeton

E/A-Module – Überblick

Die POINT Guard I/O-Module implementieren die Erweiterungen des CIP Safety-Protokolls zu EtherNet/IP- und DeviceNet-Netzwerken und bieten zahlreiche Leistungsmerkmale für ein Sicherheitssystem.

Verwenden Sie die Module, um ein Netzwerksystem mit Sicherheitssteuerung zu erstellen, das die Anforderungen bis SIL 3, wie in IEC 61508 (Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme) definiert, und die Anforderungen für Sicherheitskategorie 4 gemäß der Norm EN 13849-1 erfüllt.

Die dezentrale E/A-Kommunikation für sicherheitsrelevante E/A-Daten erfolgt über Sicherheitsverbindungen, die CIP Safety über ein EtherNet/IP- oder DeviceNet-Netzwerk unterstützen. Die Datenverarbeitung wird in der Sicherheitssteuerung ausgeführt.

Status- und Fehlerdiagnose der POINT Guard I/O-Module werden von einer Steuerung überwacht. Die folgende Liste enthält für POINT Guard I/O-Module übliche Leistungsmerkmale:

- Sicherheitseingänge
  - Sicherheitsgeräte, wie z. B. Not-Halt-Drucktasten, Gate Switches und Sicherheits-Lichtgitter können angeschlossen werden.

  - Der Zweikanalmodus bewertet die Konstanz zwischen zwei Eingangssignalen (Kanälen), was den Einsatz des Moduls für Sicherheitskategorie 3 und 4 sowie in Anwendungen ermöglicht, die bis einschließlich Leistungsstufe „e“ zugelassen sind.
  - Die Zeit einer logischen Diskrepanz zwischen zwei Kanälen kann mithilfe einer Diskrepanzzeit-Einstellung überwacht werden.
  - Einzelkanalmodus für Sicherheitsgeräte und Anwendungen, die für SIL 2 zertifiziert sind.
  - Eine externe Kurzschlussüberprüfung der Verdrahtung ist möglich, wenn die Eingänge in Kombination mit Testausgängen verdrahtet werden. Wenn diese Funktion verwendet wird, muss das Modul in Kombination mit Testausgängen verdrahtet werden.
  - Die unabhängig einstellbare Ein- und Ausschaltverzögerung steht für jeden Kanal zur Verfügung.
- Testausgänge (nur Eingangsmodule)
  - Separate Testausgänge stehen für die Erkennung von Kurzschlüssen eines Sicherheitseingangs (oder von Eingängen) zur Verfügung.
  - Geräte, wie beispielsweise Sicherheitssensoren, können mit Spannung (24 V) versorgt werden.
  - Testausgänge können als Standardausgänge konfiguriert werden.
  - Spezielle Testausgänge können zum Erkennen von Drahtbrüchen einer Muting-Leuchte verwendet werden.
- Sicherheitsausgänge
  - Halbleiterausgänge
    – Zweikanalmodus stellt eine redundante Steuerung mithilfe zweier Ausgangssignale (Kanäle) zur Verfügung, welche die Verwendung des Moduls für Sicherheitskategorie 3, 4 und für Anwendungen bis einschließlich Leistungsstufe „e“ ermöglicht.
    – Sicherheitsausgänge können Impulstests unterzogen werden, mit denen sich Kurzschlüsse an 24 V DC in der Feldverdrahtung erkennen lassen.
- E/A-Statusdaten – Neben E/A-Statusdaten umfasst das Modul auch Statusdaten zur Überwachung von E/A-Fehlern in den einzelnen Schaltkreisen.
- Sicherheit – Die Konfigurationsdaten des Moduls können durch ein Kennwort geschützt werden.

Architektur des Sicherheitssystems

POINT Guard I/O-Module werden in der POINT I/O-Plattform verwendet und können Sicherheitsnachrichten über Netzwerkadapter kommunizieren, um eine Verbindung zu EtherNet/IP- oder DeviceNet-Netzwerken herzustellen.

Empfohlene Adapter

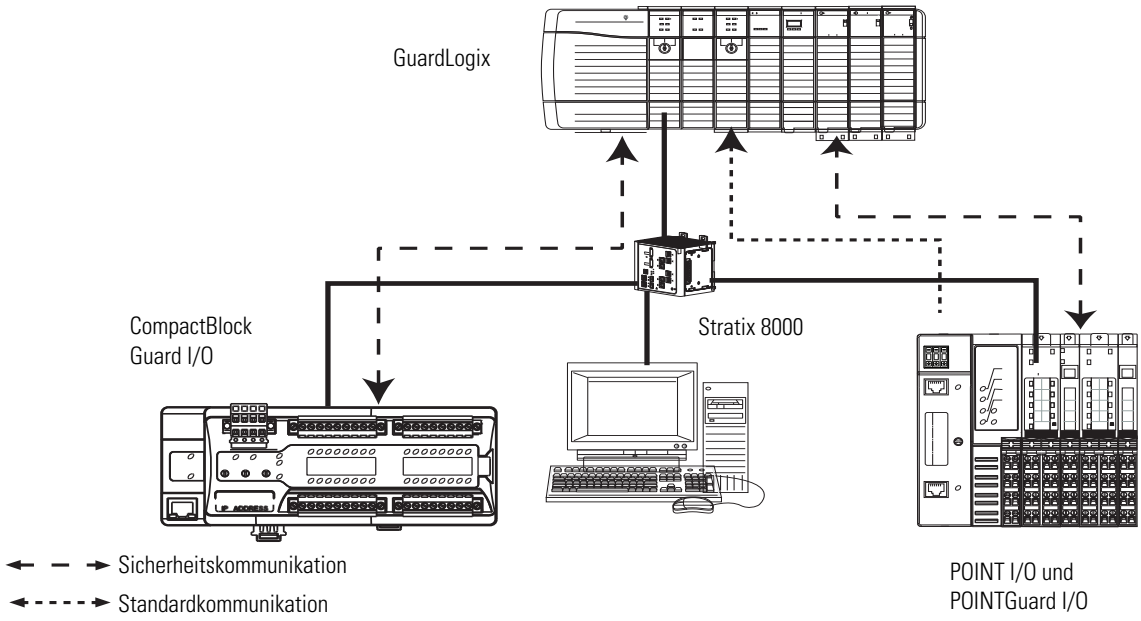
Netzwerk	System	Adapter[a]
EtherNet/IP	GuardLogix	1734-AENT
		1734-AENTR
DeviceNet	SmartGuard	1734-PDN

a. Nicht kompatibel mit 1734-ADN-, 1734-ADNX-, 1734-APB- oder 1734-ACNR-Adaptern.

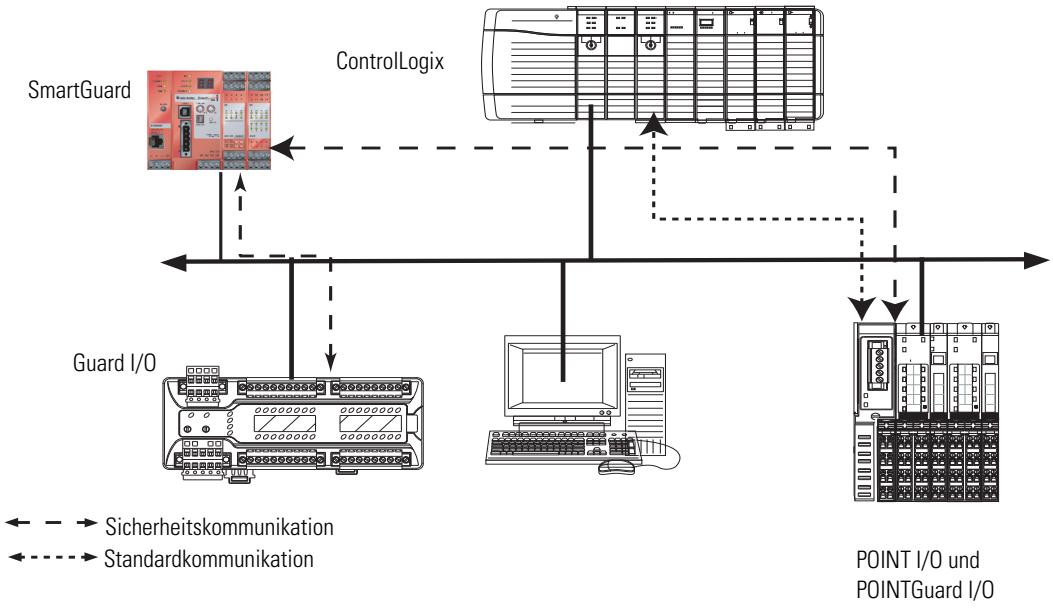
CIP Safety-Architekturen

Verwenden Sie POINT Guard I/O-Module in EtherNet/IP- oder DeviceNet-Sicherheitsarchitekturen. Die Sicherheitsausgänge werden über Sicherheitssteuerungen gesteuert. Die Standardausgänge können über Sicherheits- oder Standardsteuerungen gesteuert werden.

POINT Guard I/O-Module in der EtherNet/IP-Sicherheitsarchitektur



POINT Guard I/O-Module in DeviceNet-Sicherheitsarchitekturen



Anforderungen an Sicherheitsanwendungen

Das POINT Guard I/O-System wurde für die Verwendung in Sicherheitsanwendungen bis einschließlich SIL 3 (Sicherheitsintegritätsstufe 3) und Kategorie (CAT) 4 zertifiziert, in denen der ausgeschaltete Zustand der sichere Zustand ist. Die Anforderungen an die Sicherheitsanwendungen umfassen die Beurteilung der Versagenswahrscheinlichkeit (Versagenswahrscheinlichkeit bei Anforderung und Versagenswahrscheinlichkeit pro Stunde), die Einstellungen der Systemreaktionszeit und funktionale Verifizierungstests, die SIL3-Kriterien erfüllen.

Informationen zu den Anforderungen an Sicherheitssysteme, einschließlich funktionaler Validierungstestintervalle, Systemreaktionszeit und Berechnungen der Versagenswahrscheinlichkeit finden Sie in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch. Sie müssen diese Anforderungen vor dem Inbetriebnehmen eines POINT Guard I/O-System gelesen, verstanden und erfüllt haben.

Sicherheitsnetzwerknummer

Informationen zur Sicherheitsnetzwerknummer finden Sie in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

Sicherheitssignatur

Sicherheitssignaturen werden von der Sicherheitssteuerung erstellt. Die Sicherheitssignatur besteht aus einer ID-Nummer, einem Datum und der Uhrzeit. Diese Daten identifizieren den Sicherheitsteil eines Projekts eindeutig. Hierzu gehören die gesamte Sicherheitslogik und -konfiguration sowie alle Sicherheitsdaten. Die POINT Guard I/O-Module verwenden die Sicherheitssignatur, um die Projektintegrität zu bestimmen und um sicherstellen zu können, dass das richtige Projekt auf die Zielsteuerung heruntergeladen wurde.

Das Erstellen, Aufzeichnen und Verifizieren der Sicherheitssignatur ist beim Entwickeln einer Sicherheitsanwendung obligatorisch.

Ausführliche Informationen hierzu finden Sie in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

Sicherheitsfunktionen

Thema	Seite
Einleitung	23
E/A-Sicherheitsmodule	23
Sicherheitseingänge	24
Sicherheitsausgänge	32
E/A-Statusdaten	34
Anforderungen für Steuergeräte	35
Sicherheitsmaßnahmen	36
Gesetzgebung und Industrienormen	36

Einleitung

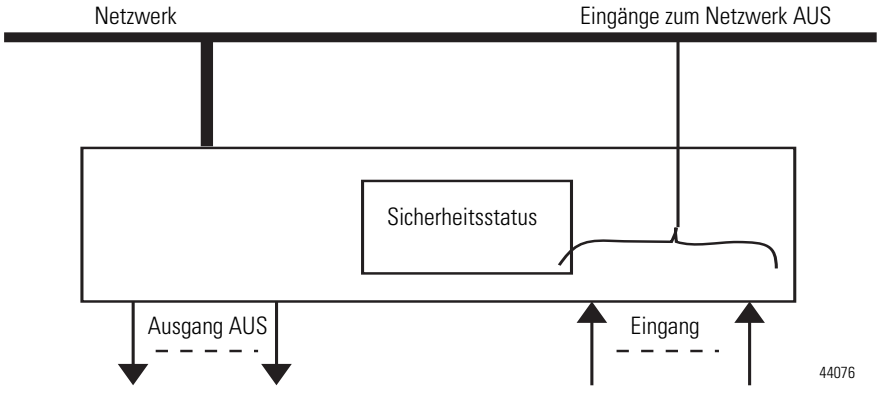
Dieses Kapitel enthält wichtige Informationen zu den Sicherheitsfunktionen der Module. Lesen Sie außerdem den kurzen Überblick zu internationalen Normen und Richtlinien.

E/A-Sicherheitsmodule

Die POINT Guard I/O-Module stellen folgende Sicherheitszustände zur Verfügung:

- Sicherheitsausgänge: Aus
- Sicherheitseingangsdaten für das Netzwerk: Aus (einkanalig und zweikanalig sind gleichwertig)

Sicherheitsstatus



Das Modul wurde für den Einsatz in Anwendungen konzipiert, in denen der AUS-Zustand der Sicherheitszustand ist.

Sicherheitseingänge

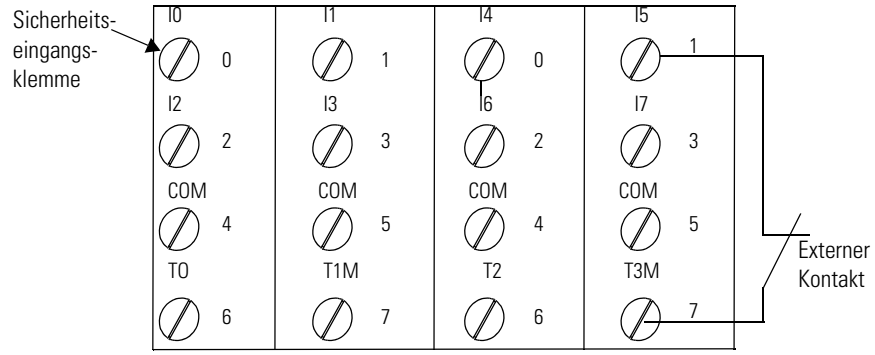
Dieser Abschnitt enthält Informationen zu den Sicherheitseingängen und den diesen zugeordneten Testausgängen. Ein Sicherheitseingang kann optional mit Testausgängen verwendet werden. Sicherheitseingänge werden zum Überwachen der Sicherheitseingangsgeräte verwendet.

Verwenden eines Testausgangs mit einem Sicherheitseingang

Ein Testausgang kann in Kombination mit einem Sicherheitseingang zur Erkennung von Kurzschlüssen, kanalübergreifenden Fehlern und Fehlern aufgrund von Drahtbrüchen verwendet werden. Konfigurieren Sie den Testausgang als Impulstestquelle, und ordnen Sie ihn einem bestimmten Sicherheitseingang zu.

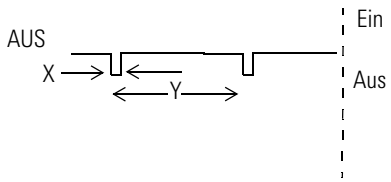
TIPP Der Testausgang kann auch als 24-V-DC-Spannungsversorgung für ein externes Gerät konfiguriert werden, z. B. für ein Lichtgitter.

Beispielverwendung eines POINT Guard I/O-Eingangsmoduls



Dabei gilt:
T0 = Testausgang 0
T1M = Testausgang 1 mit Muting
T2 = Testausgang 2
T3M = Testausgang 3 mit Muting
I0–I7 = Sicherheitseingänge

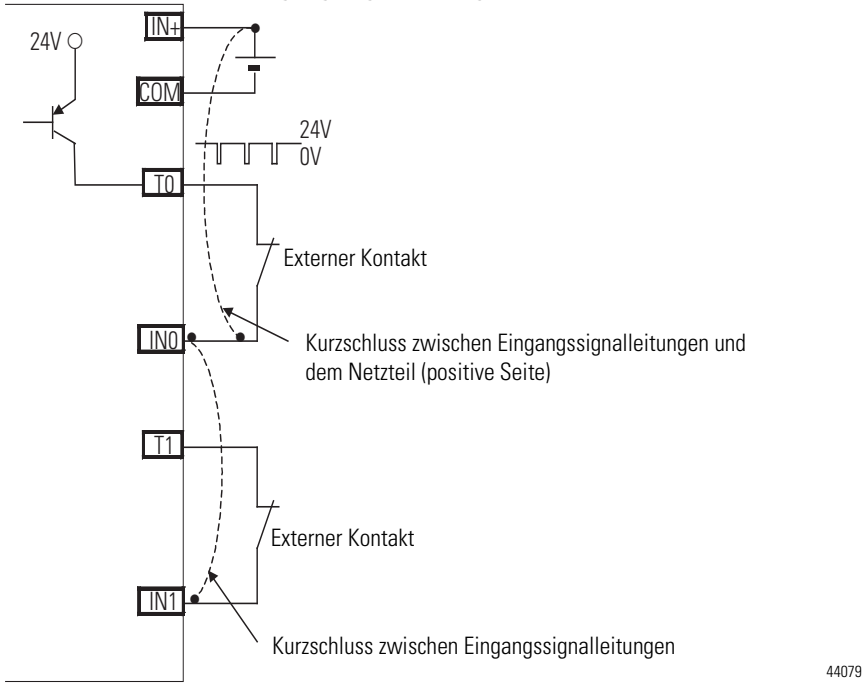
Testimpuls in einem Zyklus



Das 1734-IB8S-Modul hat eine typische Impulsdauer (X) von 525 µs. Der Impulszeitraum (Y) ist typischerweise 144 ms.

Beim Schließen des externen Eingangskontakts wird ein Testimpuls über die Testausgangsklemme ausgegeben, um die Feldverdrahtung und die Eingangsschaltung zu überprüfen. Mit dieser Funktion können Kurzschlüsse zwischen Eingängen und der 24-V-Stromversorgung und sowie zwischen den Eingangssignalleitungen erkannt werden. Außerdem werden Drahtbrüche erkannt.

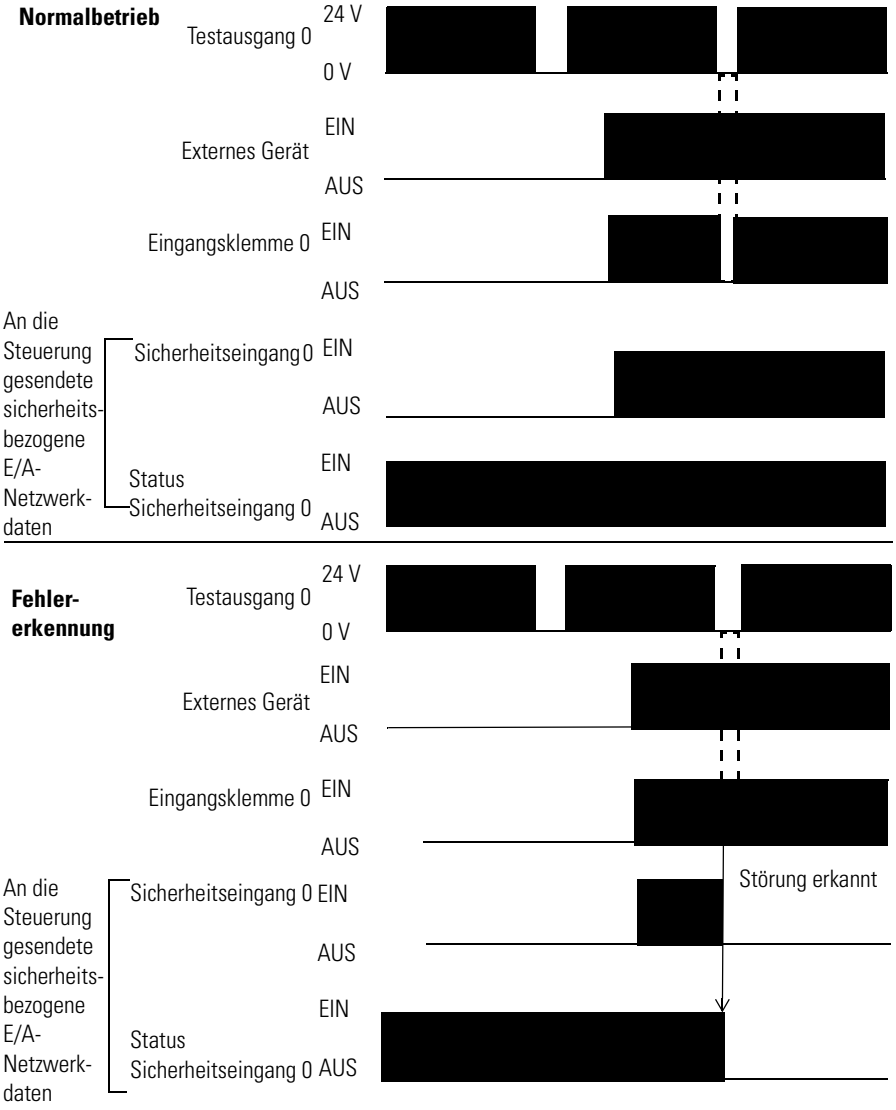
Kurzschluss zwischen Eingangssignalleitungen



Einzelkanalmodus

Falls ein Fehler erkannt wird, werden die Sicherheitseingangsdaten und der Sicherheitseingangsstatus deaktiviert.

Normalbetrieb und Fehlererkennung (nicht maßstabsgetreu)



Zweikanalmodus und Diskrepanzzeit

Zur Unterstützung zweikanaliger Sicherheitsgeräte kann die Konsistenz zwischen Signalen auf zwei Kanälen beurteilt werden. Die Signale können entweder als gleichwertig oder komplementär eingestuft werden. Diese Funktion überwacht, wie lange eine Diskrepanz zwischen den beiden Kanälen vorliegt.

Falls die Länge der Diskrepanz die konfigurierte Diskrepanzzeit überschreitet (0–65 530 ms in Inkrementen von 10 ms) werden die Sicherheitseingangsdaten und der individuelle Sicherheitseingangsstatus für beide Kanäle deaktiviert.

WICHTIG Die zweikanalige Funktion wird mit zwei aufeinander folgenden Eingängen verwendet, die paarweise angeordnet sind, beginnend mit einer geraden Eingangsnummer, wie z. B. Eingänge 0 und 1, 2 und 3 usw.

WICHTIG Zweck der Diskrepanzzeit ist es, normale Differenzen zwischen der Kontaktschaltung zuzulassen, wenn Anforderungen an Sicherheitseingänge gesendet werden. Damit diese Tests ordnungsgemäß funktionieren, wird während der Diskrepanzzeit nur eine Anforderung am Sicherheitseingang erwartet. Falls der Wert für die Diskrepanzzeit zu hoch ist und während dieser Zeit mehrere Anforderungen auftreten, weisen beide Sicherheitseingangskanäle einen Fehler auf.

In der folgenden Tabelle ist die Beziehung zwischen den Zuständen der Eingangsklemmen und den Eingangsdaten bzw. dem Eingangsstatus der Steuerung veranschaulicht.

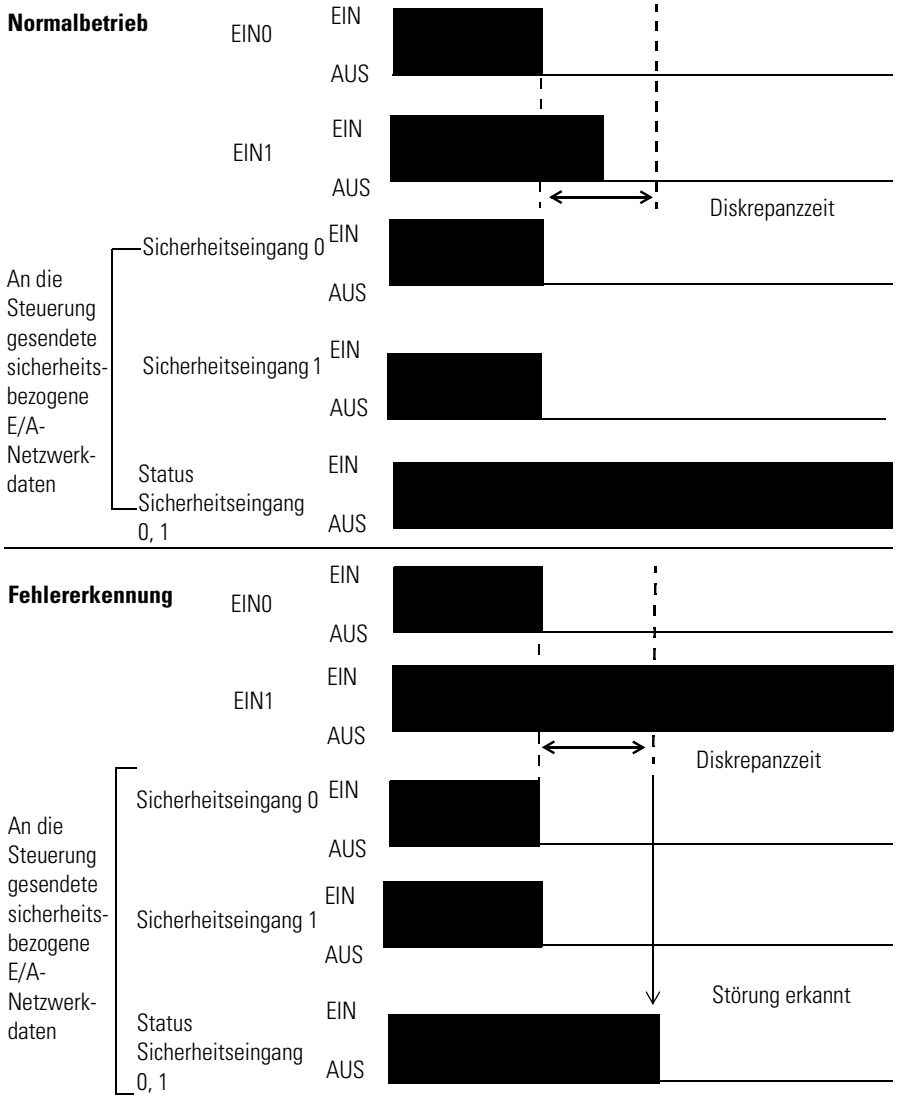
Eingangsstatus der Klemmen und E/A-Daten der Steuerung

Zweikanalmodus	Eingangs-klemme		Eingangsdaten und -status der Steuerung				Resultierende Daten bei zwei Kanälen	Resultierender Status bei zwei Kanälen
	EIN0	EIN1	Daten Sicherheits-eingang 0	Daten Sicherheits-eingang 1	Status Sicherheits-eingang 0	Status Sicherheits-eingang 1		
Zwei Kanäle, gleichwertig	AUS	AUS	AUS	AUS	EIN	EIN	AUS	Normal
	AUS	EIN	AUS	AUS	AUS	AUS	AUS	Fehler
	EIN	AUS	AUS	AUS	AUS	AUS	AUS	Fehler
	EIN	EIN	EIN	EIN	EIN	EIN	EIN	Normal
Zwei Kanäle, komplementär	AUS	AUS	AUS	EIN	AUS	AUS	AUS	Fehler
	AUS	EIN	AUS	EIN	EIN	EIN	AUS	Normal
	EIN	AUS	EIN	AUS	EIN	EIN	EIN	Normal
	EIN	EIN	AUS	EIN	AUS	AUS	AUS	Fehler

Zwei Kanäle, gleichwertig

Im gleichwertigen Modus müssen beide Eingänge eines Paars denselben (gleichwertigen) Zustand aufweisen. Kommt es in einem Kanal des Paars zu einer Transition vor der Transition im zweiten Kanal des Paars, tritt eine Diskrepanz auf. Wenn der zweite Kanal vor Ablauf der Diskrepanzzeit in den entsprechenden Zustand übergeht, gelten die Eingänge als gleichwertig. Kommt es vor Ablauf der Diskrepanzzeit nicht zur zweiten Transition, wird für die Kanäle ein Fehler ausgegeben. Im Fehlerzustand werden Eingang und Status für beide Kanäle auf einen niedrigen Wert (aus) gesetzt. Wurden die Kanäle als gleichwertiges, zweikanaliges Paar konfiguriert, werden die Daten-Bits für beide Kanäle stets als gleichwertig, oder beide als hoch (1) oder niedrig (0) an die Steuerung gesendet.

Gleichwertig, Normalbetrieb und Fehlererkennung (nicht maßstabsgetreu)

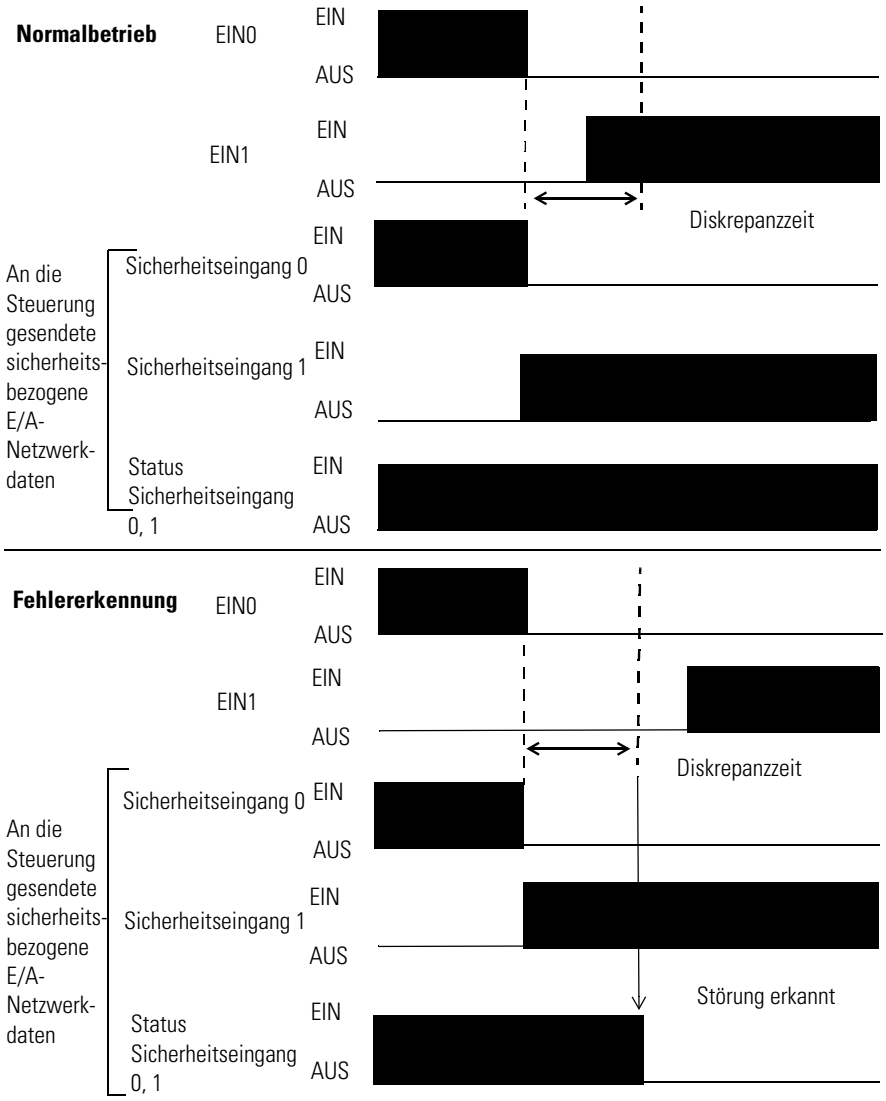


Zwei Kanäle, komplementär

Im komplementären Modus müssen die Eingänge eines Paars den entgegengesetzten (komplementären) Zustand aufweisen. Kommt es in einem Kanal des Paars zu einer Transition vor der Transition im zweiten Kanal des Paars, tritt eine Diskrepanz auf. Wenn der zweite Kanal vor Ablauf der Diskrepanzzeit in den entsprechenden Zustand übergeht, gelten die Eingänge als komplementär.

Kommt es vor Ablauf der Diskrepanzzeit nicht zur zweiten Transition, wird für die Kanäle ein Fehler ausgegeben. Der Fehlerzustand komplementärer Eingänge liegt vor, wenn der Eingang mit der geraden Zahl ausgeschaltet und der Eingang mit der ungeraden Zahl eingeschaltet ist. Im Fehlerzustand sind beide Kanalstatus-Bits auf niedrig gesetzt. Wurden die Kanäle als komplementäres, zweikanaliges Paar konfiguriert, werden die Daten-Bits für beide Kanäle stets an die Steuerung im komplementären oder gegensätzlichen Zustand gesendet.

Komplementär, Normalbetrieb und Fehlererkennung (nicht maßstabsgetreu)



Wiederherstellung nach einem Fehler des Sicherheitseingangs

Falls ein Fehler erkannt wird, bleiben die Sicherheitseingangsdaten im AUS-Zustand. Gehen Sie wie folgt vor, um die Daten des Sicherheitseingangs erneut zu aktivieren.

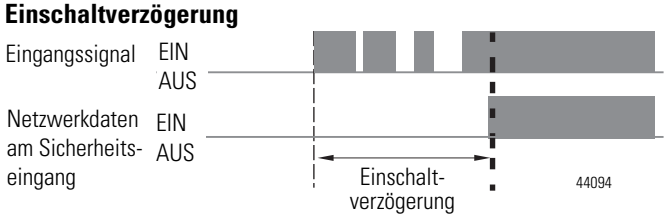
1. Beheben Sie die Ursache des Fehlers.
2. Bringen Sie den Sicherheitseingang (oder die Sicherheitseingänge) in den sicheren Zustand.
3. Warten Sie, bis die Selbsthaltezeit für Eingangsfehler abgelaufen ist.

   Nachdem diese Schritte ausgeführt wurden, wird die E/A-Anzeige (rot) ausgeschaltet. Die Eingangsdaten sind jetzt aktiv.

Eingangsverzögerungen

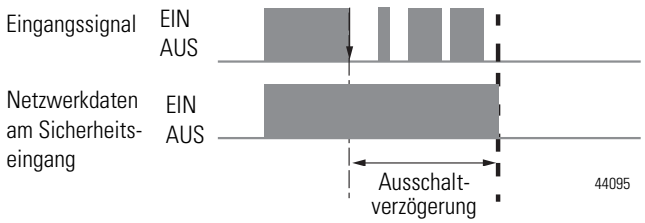
Einschaltverzögerung – Ein Eingangssignal wird während der Einschaltverzögerungszeit und nach der ansteigenden Flanke des Eingangskontakts als logische 0 behandelt (0–126 ms, in Inkrementen von 6 ms). Der Eingang wird nur eingeschaltet, wenn der Eingangskontakt nach Ablauf der Einschaltverzögerungszeit aktiviert bleibt. Auf diese Weise können schnelle Änderungen der Eingangsdaten aufgrund von Kontaktprellen verhindert werden.

Einschaltverzögerung



Ausschaltverzögerung – Ein Eingangssignal wird während der Ausschaltverzögerungszeit und nach der abfallenden Flanke des Eingangskontakts als logische 1 behandelt (0–126 ms, in Inkrementen von 6 ms). Der Eingang wird nur ausgeschaltet, wenn der Eingangskontakt nach Ablauf der Ausschaltverzögerungszeit deaktiviert bleibt. Auf diese Weise können schnelle Änderungen der Eingangsdaten aufgrund von Kontaktprellen verhindert werden.

Ausschaltverzögerung



Sicherheitsausgänge

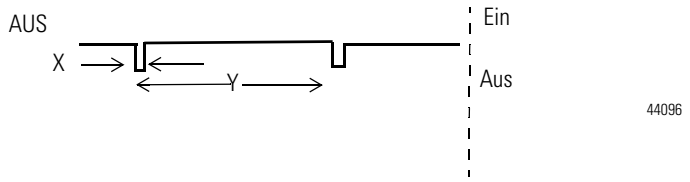
Dieser Abschnitt enthält Informationen zu Sicherheitsausgängen.

Sicherheitsausgang mit Testimpuls

Wenn der Sicherheitsausgang eingeschaltet ist, kann der Sicherheitsausgang so konfiguriert werden, dass er einen Impulstest für den Sicherheitsausgangskanal vornimmt.

Mit dieser Funktion können Kurzschlüsse zwischen Ausgangssignalleitungen und dem Netzteil (positive Seite) sowie Kurzschlüsse zwischen den Ausgangssignalleitungen selbst erkannt werden. Falls ein Fehler erkannt wird, werden die Sicherheitsausgangsdaten und der Status der einzelnen Sicherheitsausgänge deaktiviert.

Testimpuls in einem Zyklus



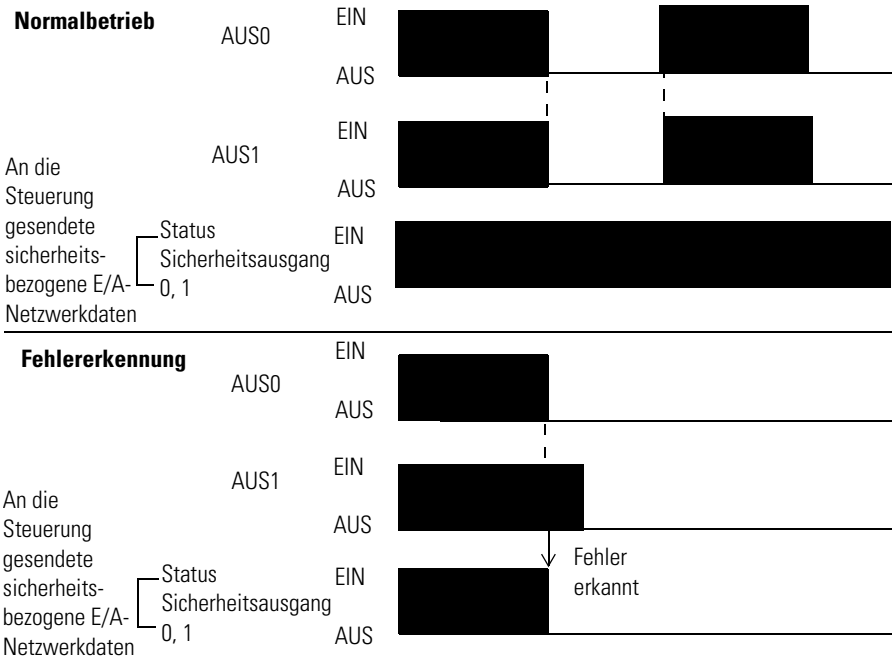
Das 1734-OB8S-Modul hat eine typische Impulsdauer (X) von 475 µs. Der Impulszeitraum (Y) beträgt typischerweise 575 ms.

WICHTIG Damit der Testimpuls keine Fehlfunktion des angeschlossenen Geräts auslöst, müssen Sie sorgfältig auf die Eingangsreaktionszeit des Ausgangsgeräts achten.

Zweikanalige Einstellung

Wenn sich die Daten beider Kanäle im EIN-Zustand befinden und keiner der Kanäle fehlerhaft ist, werden die Ausgänge eingeschaltet. Der Status ist normal. Falls an einem der Kanäle ein Fehler erkannt wird, werden die Sicherheitsausgangsdaten und der Status der einzelnen Sicherheitsausgänge für beide Kanäle ausgeschaltet.

Zweikanalige Einstellung (nicht maßstabsgetreu)



Wiederherstellung nach einem Fehler des Sicherheitsausgangs

Falls ein Fehler erkannt wird, werden die Sicherheitsausgänge ausgeschaltet und bleiben im AUS-Zustand. Gehen Sie wie folgt vor, um die Daten des Sicherheitsausgangs erneut zu aktivieren.

1. Beheben Sie die Ursache des Fehlers.
2. Bringen Sie den Sicherheitsausgang (oder die Sicherheitsausgänge) in den Sicherheitszustand.
3. Warten Sie, bis die Selbsthaltezeit für Ausgangsfehler abgelaufen ist.

Nachdem diese Schritte ausgeführt wurden, wird die E/A-Anzeige (rot) ausgeschaltet. Die Ausgangsdaten können jetzt gesteuert werden.

WICHTIG Blockierende höherwertige Fehler können nur durch Aus- und erneutes Einschalten des Moduls gelöscht werden.

E/A-Statusdaten

Neben den E/A-Daten stellt das Modul auch Statusdaten zur Überwachung der E/A-Schaltkreise zur Verfügung. Der Status umfasst die folgenden Daten, die von den Steuerungen gelesen werden können. Hinweis: 1 = EIN/Normal und 0 = AUS/Fehler/Alarm:

- Status individueller Eingangspunkte
- Kombinierter Eingangsstatus
- Status individueller Ausgangspunkte
- Kombinierter Ausgangsstatus
- Status individueller Testausgänge
- Individuelle Ausgangsüberwachung (tatsächlicher EIN/AUS-Zustand der Ausgänge)

Der Status individueller Punkte weist darauf hin, ob die einzelnen Sicherheitseingänge, Sicherheitsausgänge oder Testausgänge normal sind (normaler Status: EIN, fehlerhafter Status: AUS). Bei schwerwiegenden Fehlern sind eventuell Kommunikationsverbindungen unterbrochen, sodass die Statusdaten nicht gelesen werden können. Status-Bits sind in der Steuerungsdatentabelle deaktiviert (AUS), wenn die Verbindung unterbrochen wurde.

Der kombinierte Status wird durch ein UND des Status aller Sicherheitseingänge oder aller Sicherheitsausgänge zur Verfügung gestellt. Wenn alle Eingänge oder Ausgänge den Normalzustand aufweisen, lautet der kombinierte Status EIN. Wenn mindestens einer der Eingänge oder Ausgänge einen Fehler aufweist, lautet der entsprechend kombinierte Status AUS. Dieser wird auch kombinierter Sicherheitseingangsstatus oder kombinierter Sicherheitsausgangsstatus genannt.

Anforderungen für Steuergeräte

Die folgende Tabelle enthält Informationen zu Steuergeräten.

ACHTUNG

Verwenden Sie ausschließlich Komponenten und Geräte, die den einschlägigen Sicherheitsstandards für die erforderlichen Sicherheitskategorien (SIL) entsprechen. Die Einhaltung der Anforderungen der jeweiligen Sicherheitskategorie (SIL) muss als ganzes System bestimmt werden. Wir empfehlen, die Einhaltung der erforderlichen Sicherheitsstufe durch eine geeignete Zertifizierungsgesellschaft bestätigen zu lassen.

Anforderungen für Steuergeräte

Gerät	Anforderung	Sicherheitskomponenten der Allen-Bradley-Serie
Not-Halt-Schalter	Verwenden Sie zugelassene Geräte mit Direktöffnungsmechanismen, die IEC/EN 60947-5-1 entsprechen.	Serie 800F, 800T
Türverriegelungsschalter, Endschalter	Verwenden Sie zugelassene Geräte mit Direktöffnungsmechanismen, die IEC/EN 60947-5-1 entsprechen und Mikrolasten von 24 V DC bei 3 mA schalten können.	Serie 440K, 440G, 440H für Verriegelungsschalter Serie 440P, 802T für Endschalter
Sicherheitssensoren	Verwenden Sie zugelassene Geräte, die den einschlägigen Produktnormen, Richtlinien und Regeln im Einsatzland entsprechen.	Alle Guardmaster-Produkte
Relais mit zwangsgeführten Kontakten, Schütze	Verwenden Sie zugelassene Geräte mit zwangsgeführten Kontakten, die EN 50205 entsprechen. Verwenden Sie für Rückführungszwecke Geräte mit Kontakten, die Mikrolasten von 24 V DC bei 3 mA schalten können.	Serie 700S, 100S
Andere Geräte	Überprüfen Sie, ob die verwendeten Geräte die Anforderungen der jeweiligen Sicherheitskategorien erfüllen.	–

Sicherheitsmaßnahmen

ACHTUNG

Ein Verlust der erforderlichen Sicherheitsfunktion kann zu ernsthaften Verletzungen führen. Befolgen Sie daher diese Sicherheitsmaßnahmen:

- Verwenden Sie die Testausgänge der Module nicht als Sicherheitsausgänge.
- Verwenden Sie keine standardmäßigen EtherNet-, DeviceNet- oder ControlNet-E/A-Daten oder explizite Nachrichtendaten als Sicherheitsdaten.
- Verwenden Sie keine LED-Statusanzeigen an den E/A-Modulen für Sicherheitsvorgänge.
- Schließen Sie keine die Nennwerte überschreitenden Lasten an die Sicherheitsausgänge an.
- Verdrahten Sie die POINT Guard I/O-Module ordnungsgemäß, sodass die 24-V-DC-Leitung die Sicherheitsausgänge weder unbeabsichtigt noch versehentlich berührt.
- Löschen Sie vorherige Konfigurationsdaten, bevor Sie Geräte am Netzwerk anschließen.
- Legen Sie eindeutige Netzwerkknotenadressen fest, bevor Sie Geräte am Netzwerk anschließen.
- Führen Sie vor der Inbetriebnahme des Systems Tests aus, um sicherzustellen, dass Gerätekonfiguration und Betrieb korrekt sind.
- Wenn Sie ein Gerät ersetzen, konfigurieren Sie das Austauschgerät entsprechend, und stellen Sie sicher, dass es ordnungsgemäß funktioniert.
- Beim Installieren oder Ersetzen von Modulen müssen alle vorherigen Konfigurationen gelöscht werden, bevor Eingangs- oder Ausgangsleistung am Gerät angeschlossen wird.

Gesetzgebung und Industrienormen

Lesen Sie diesen Abschnitt, um sich mit der geltenden Gesetzgebung und den Industrienormen vertraut zu machen. Beispiele für relevante internationale Industrienormen:

- IEC 61508 (SIL 1-3)
- IEC 61131-2
- IEC 60204-1
- IEC 61000-6-2
- IEC 61000-6-4
- IEC 62061
- ISO 13849-1

Die Module erhielten von der ODVA die Zertifizierung „DeviceNet Safety Conformance Test“, sofern die Produkte entsprechend gekennzeichnet sind.

Europa

Die Typengenehmigung des TÜV-Rheinland betrifft die Einhaltung der anwendbaren Anforderungen folgender Normen:

- Europäische Industrienormen
  - IEC 61508 (SIL1-3)
  - IEC 61131-2
  - EN 60204-1
  - EN/IEC 62061
  - ISO 13849-1 (PL a, b, c, d, e)

Europäische Zulassung für explosionsgefährdete Standorte

Europäische Zertifizierung für Zone 2 (Die folgenden Informationen gelten, wenn das Produkt mit dem Ex- oder EEx-Zeichen gekennzeichnet ist.)

Dieses Gerät ist für die Verwendung an explosionsgefährdeten Standorten gemäß der EU-Richtlinie 94/9/EG vorgesehen und wurde als konform mit den grundlegenden Gesundheits- und Sicherheitsanforderungen hinsichtlich des Designs und Aufbaus von Geräten der Kategorie 3 bewertet, die für die Verwendung an potenziell explosionsgefährdeten Standorten gemäß Anhang II dieser Richtlinie vorgesehen sind. Die Übereinstimmung mit den grundlegenden Gesundheits- und Sicherheitsanforderungen wurde durch die Konformität mit EN 60079-15 und EN 60079-0 versichert.

WARNUNG

- Dieses Gerät darf nicht direktem Sonnenlicht oder anderen Quellen mit UV-Strahlung ausgesetzt werden.
- Das Gerät muss in einem Gehäuse installiert werden, um mindestens IP54-Schutz zur bieten, wenn es in Umgebungen der Zone 2 eingesetzt wird.
- Dieses Gerät muss innerhalb der von Allen-Bradley definierten Bemessungswerte verwendet werden.
- Es müssen Vorsichtsmaßnahmen getroffen werden, um ein Überschreiten der Bemessungsspannung durch Einschwingstörungen von mehr als 40 % zu verhindern, wenn das Gerät in Umgebungen der Zone 2 eingesetzt wird.
- Sichern Sie alle externen Verbindungen zu diesem Gerät mit Schrauben, Schiebeverriegelungen, Gewindeanschlüssen oder anderen Vorrichtungen, die mit diesem Produkt geliefert werden.
- Ziehen Sie die Geräte nur ab, wenn das Gerät ausgeschaltet ist oder der Bereich als nicht explosionsgefährdet gilt.

EU-Richtlinien

Diese Produkte erfüllen die Anforderungen der EMV-Richtlinie und der Niederspannungsrichtlinie, sofern anwendbar. Weitere Informationen finden Sie in den entsprechenden Installationsanleitungen.

EMV-Richtlinie

Rockwell Automation-Geräte, die die Anforderungen der EU-Richtlinien erfüllen, entsprechen auch den anwendbaren EMV-Normen, damit sie einfacher in andere Geräte oder in eine ganze Maschine eingebaut werden können. Die aktuellen Produkte wurden auf die Einhaltung der EMV-Normen geprüft. Ob sie jedoch auch in dem vom Kunden verwendeten System den Normen entsprechen, muss vom Kunden überprüft werden.

Die EMV-abhängige Leistung von Rockwell Automation-Geräten, die den Anforderungen der EMV-Richtlinie entsprechen, variieren abhängig von der Konfiguration, Verdrahtung und von anderen Bedingungen der Anlagen oder Schaltschränke, in denen die Rockwell Automation-Geräte installiert werden. Der Kunde muss daher eine Endprüfung vornehmen, um sicherzustellen, dass die Geräte und die gesamte Maschine den EMV-Normen entsprechen.

Nordamerika

In Nordamerika umfasst der Zulassungstyp des TÜV Rheinland die Einhaltung relevanter Industrienormen durch Guard I/O-Produkte sowie weiterführende Informationen wie zum Beispiel Folgendes:

- US-Industrienormen – ANSI RIA15.06, ANSI B11.19, NFPA 79
- Die Module erhielten die UL-Eintragung gemäß den Industrienormen der USA und von Kanada, sofern das Produkt entsprechend gekennzeichnet ist.

Nordamerikanische Zulassung für explosionsgefährdete Standorte

Die folgenden Informationen treffen zu, wenn dieses Gerät an explosionsgefährdeten Standorten eingesetzt wird.	**Informations sur l'utilisation de cet équipement en environnements dangereux.**
Produkte, die mit „CL I, DIV 2, GP A, B, C, D" gekennzeichnet sind, eignen sich nur für den Einsatz an explosionsgefährdeten Standorten der Klasse I, Division 2, Gruppen A, B, C, D und an nicht explosionsgefährdeten Standorten. Jedes Produkt wird mit Kennzeichnungen auf dem Zulassungstypenschild geliefert, auf dem der Temperaturcode für den explosionsgefährdeten Standort angegeben ist. Werden Produkte innerhalb eines Systems kombiniert, kann anhand des ungünstigsten Temperaturcodes (niedrigste „T"-Zahl) der Temperaturcode für das gesamte Systems bestimmt werden. Kombinationen von Geräten in Ihrem System müssen von den lokalen zuständigen Behörden zum Zeitpunkt der Installation überprüft werden.	Les produits marqués „CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.

WARNUNG	**EXPLOSIONSGEFAHR –** • Ziehen Sie die Geräte nur ab, wenn das Gerät ausgeschaltet oder der Bereich bekanntermaßen nicht explosionsgefährdet ist. • Trennen Sie Verbindungen zu diesen Geräten nur, wenn das Gerät ausgeschaltet ist oder der Bereich als nicht explosionsgefährdet gilt. Sichern Sie alle externen Verbindungen, die an diesem Gerät angeschlossen werden, mit Schrauben, Schiebeverriegelungen, Gewindeanschlüssen oder anderen Vorrichtungen, die mit diesem Produkt geliefert werden. • Durch den Austausch von Komponenten ist das Gerät eventuell nicht mehr für Klasse I, Division 2 geeignet. • Falls das Produkt Batterien enthält, dürfen diese nur in einem Bereich ausgetauscht werden, der bekanntermaßen nicht explosionsgefährdet ist.	**ADVERTISSEMENT**	**RISQUE D'EXPLOSION –** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

Japan

In Japan sind die Typprüfungsanforderungen in Artikel 44 des Gesetzes für Sicherheit und Gesundheit in Industrieumgebungen dargelegt. Diese Anforderungen gelten für ganze Systeme und können nicht auf ein einzelnes Modul angewandt werden. Wenn Sie also das Modul in Japan als Sicherheitsgerät für Pressen oder Scherwerkzeuge gemäß Artikel 42 des oben genannten Gesetzes einsetzen möchten, müssen Sie eine Prüfung des gesamten Systems beantragen.

Notizen:

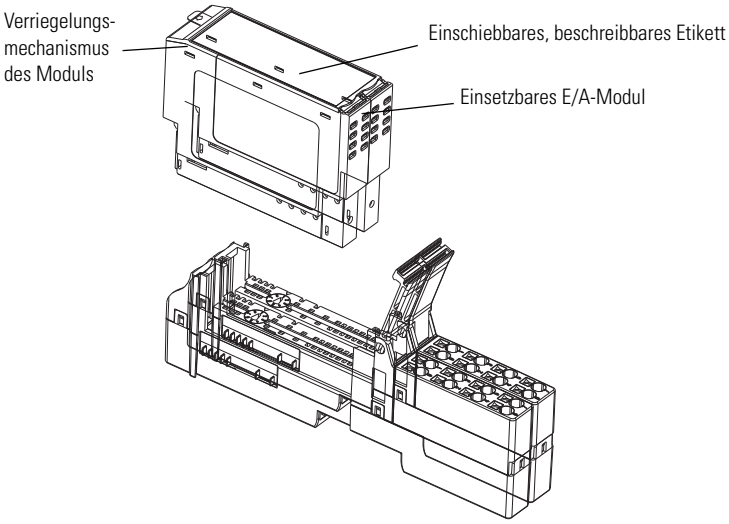
Installation des Moduls

Thema	Seite
Einleitung	43
Umgebung und Gehäuse	44
Verhinderung elektrostatischer Entladung	45
Installieren des Montagesockels	46
Anschließen des Moduls am Montagesockel	48
Anschließen der abnehmbaren Klemmenleiste	49
Ausbauen eines Montagesockels	50
Verdrahten der Module	50
Festlegen der Netzknotenadresse eines POINT Guard I/O-Moduls	52
Zurücksetzen der POINT Guard I/O-Module auf die Werkseinstellungen	55
Automatische Adressierung mit einem 1734-PDN-Adapter und mit POINT Guard I/O-Modulen	56

Einleitung

Gehen Sie wie folgt vor, um die Module zu installieren.

1. Installieren des Montagesockels.
2. Anschließen des Moduls am Montagesockel.
3. Anschließen der abnehmbaren Klemmenleiste.
4. Verdrahten der Module.



31867-M

Umgebung und Gehäuse

ACHTUNG

Dieses Gerät ist zur Verwendung in einer Industrieumgebung mit Verschmutzungsgrad 2, in Anwendungen der Überspannungskategorie II (gemäß IEC 60664-1) und in Aufstellhöhen von bis zu 2000 m ohne Herabsetzung der Betriebswerte vorgesehen.

Dieses Gerät gilt gemäß IEC/CISPR als industrielles Gerät der Gruppe 1, Klasse A. Ohne entsprechende Vorsichtsmaßnahmen kann es aufgrund von leitungsgeführten und abgestrahlten Störungen zu Schwierigkeiten hinsichtlich der elektromagnetischen Verträglichkeit in Wohngebäuden oder anderen Umgebungen kommen.

Das Gerät wird als offenes Gerät geliefert. Es muss in ein Gehäuse eingebaut werden, das für die jeweiligen Umgebungsbedingungen geeignet ist und dessen Konstruktion den Kontakt des Bedienpersonals mit stromführenden Teilen und mögliche daraus resultierende Körperverletzungen verhindert. Das Gehäuse muss über geeignete flammhemmende Eigenschaften verfügen, um die Ausbreitung von Flammen zu verhindern oder zu minimieren. Besteht das Gehäuse nicht aus Metall, muss die Flammenausbreitungskategorie 5VA, V2, V1, V0 (oder eine gleichwertige Kategorie) erfüllt sein. Das Innere des Gehäuses darf nur mithilfe eines Werkzeugs zugänglich sein. Die folgenden Abschnitte dieser Publikation können weitere Informationen über die Gehäuseschutzklassen enthalten, die bei bestimmten Produktsicherheitszertifizierungen erforderlich sind.

Lesen Sie zusätzlich zu dieser Publikation Folgendes:

- Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Allen-Bradley-Publikation 1770-4.1 (diese enthält zusätzliche Installationsanforderungen).
- NEMA-Normen 250 und IEC 60529, sofern zutreffend. Diese enthalten Erläuterungen der Schutzgrade, die von den verschiedenen Gehäusetypen zur Verfügung gestellt werden.

Verhinderung elektrostatischer Entladung

ACHTUNG

Dieses Gerät ist empfindlich gegen elektrostatische Entladung, die interne Schäden verursachen und die normale Funktionsweise beeinträchtigen kann. Befolgen Sie beim Umgang mit diesem Gerät die folgenden Richtlinien:

- Berühren Sie einen geerdeten Gegenstand, um eventuelle elektrische Ladung abzuleiten.
- Tragen Sie ein zugelassenes Erdungsband am Handgelenk.
- Berühren Sie keine Anschlüsse oder Stifte auf den Komponentenplatinen.
- Berühren Sie keine Schaltkreiskomponenten im Innern des Geräts.
- Verwenden Sie möglichst einen vor statischen Entladungen sicheren Arbeitsplatz.
- Lagern Sie das Gerät in einer geeigneten antistatischen Verpackung, wenn Sie es nicht verwenden.

WARNUNG

Wenn Sie die abnehmbare Klemmenleiste anschließen oder trennen, solange die feldseitige Spannungsversorgung angeschlossen ist, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Vergewissern Sie sich, bevor Sie fortfahren, dass keine Spannung anliegt oder dass es sich um einen nicht explosionsgefährdeten Standort handelt.

WARNUNG

Wenn Sie die Verdrahtung anschließen oder trennen, während die feldseitige Spannungsversorgung eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Vergewissern Sie sich, bevor Sie fortfahren, dass keine Spannung anliegt oder dass es sich um einen nicht explosionsgefährdeten Standort handelt.

ACHTUNG

Personal, das für die Anwendung sicherheitsbezogener programmierbarer elektronischer Systeme (PES) verantwortlich ist, muss sich der sicherheitstechnischen Anforderungen bei der Anwendung des Systems bewusst sein und für die Verwendung des Systems geschult sein.

ACHTUNG

Zur Übereinstimmung mit der CE-Niederspannungsrichtlinie müssen dieses Gerät und alle angeschossenen E/A-Module mit Sicherheits-Kleinspannung (SELV) oder mit Schutz-Kleinspannung (PELV) versorgt werden.

ACHTUNG

Dieses Produkt ist über die DIN-Schiene an der Chassiserdung geerdet. Verwenden Sie verzinkte, gelbchromatierte Stahl-DIN-Schienen, um die ordnungsgemäße Erdung sicherzustellen. Die Verwendung anderer Materialien für die DIN-Schienen (z. B. Aluminium oder Kunststoff), die korrodieren, oxidieren oder schlecht leiten, können zu einer nicht ordnungsgemäßen oder unstetigen Erdung führen. Befestigen Sie die DIN-Schiene an der Montageoberfläche etwa alle 200 mm, und verwenden Sie entsprechende Endverankerungen.

Installieren des Montagesockels

Der Montagesockel besteht aus einer einteiligen Klemmeneinheit oder einer Baugruppe mit einem Montagesockel und einer abnehmbaren Klemmenleiste. POINT Guard I/O-Module belegen zwei Sockel.

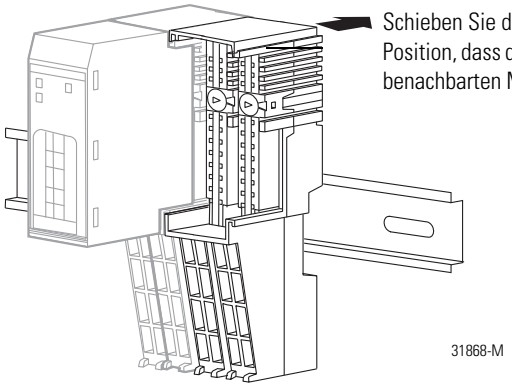
WICHTIG

Befolgen Sie beim Installieren eines Moduls folgende Richtlinien.

- Verwenden Sie das Modul in einer Umgebung, die den allgemeinen Spezifikationen entspricht.
- Verwenden Sie das Modul in einem Gehäuse gemäß IP54 (IEC 60529) oder höher.
- Verwenden Sie eine DIN-Schiene mit einer Breite von 35 mm, um die Klemmeneinheit im Schaltschrank zu befestigen.
- Platzieren Sie andere Wärmequellen in ausreichender Entfernung vom Modul, damit die für das Modul zulässigen Umgebungstemperaturen nicht überschritten werden.
- Sie können Ihr Modul horizontal oder vertikal montieren.

1. Positionieren Sie den Montagesockel wie unter Schritt 2 veranschaulicht.

2. Schieben Sie den Montagesockel nach unten, sodass die Verriegelungsseitenteile im benachbarten Modul, Netzteil oder Adapter einrasten.



3. Drücken Sie den Montagesockel fest nach unten, sodass er auf der DIN-Schiene einrastet.

Anschließen des Moduls am Montagesockel

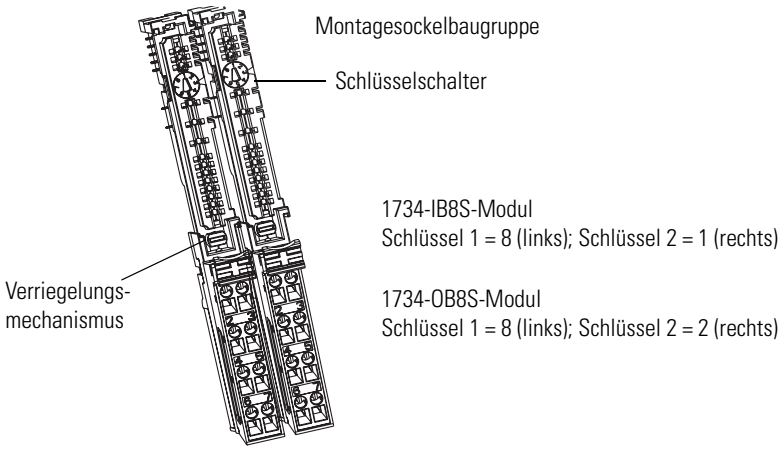
Installieren Sie das Modul vor oder nach der Installation des Montagesockels.

WARNUNG

Wenn Sie das Modul bei aktivierter Backplane einsetzen oder herausnehmen, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Vergewissern Sie sich, bevor Sie fortfahren, dass die Spannungsversorgung abgezogen ist oder dass es sich um einen nicht explosionsgefährdeten Standort handelt. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß. Verschlissene Kontakte können einen elektrischen Widerstand verursachen und den Modulbetrieb beeinträchtigen.

1. Drehen Sie die Schlüsselschalter am Montagesockel mit einem Schraubendreher im Uhrzeigersinn, bis die für den Modultyp erforderliche Zahl an der Kerbe im Sockel ausgerichtet ist.

   Notieren Sie sich, welcher Montagesockel auf der linken und rechten Seite jedes Moduls installiert wird.



2. Vergewissern Sie sich, dass sich die Klemmschraube der DIN-Schiene (orange) in der horizontalen Position befindet. Denken Sie daran, dass Sie das Modul nicht einsetzen können, wenn der Verriegelungsmechanismus des Montagesockels entriegelt ist.

3. Führen Sie das Modul gerade nach unten in die beiden nebeneinander liegenden Montagesockel ein, und drücken Sie es in Position, sodass es einrastet.

Anschließen der abnehmbaren Klemmenleiste

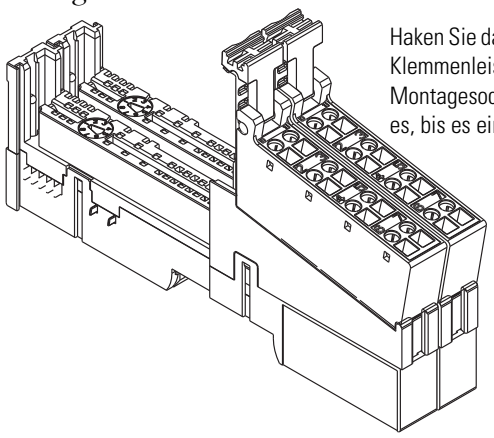
Wenn im Lieferumfang Ihrer Montagesockelbaugruppe eine abnehmbare Klemmenleiste enthalten ist, müssen Sie diese abnehmen, indem Sie diese an ihrem Griff nach oben ziehen. So können Sie den Sockel bei Bedarf abnehmen und wieder einsetzen, ohne hierfür die Verdrahtung lösen zu müssen.

WARNUNG

Wenn Sie die abnehmbare Klemmenleiste anschließen oder trennen, während feldseitige Spannung anliegt, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Vergewissern Sie sich, bevor Sie fortfahren, dass die Spannungsversorgung getrennt wurde oder dass es sich um einen nicht explosionsgefährdeten Standort handelt.

Gehen Sie wie folgt vor, um die abnehmbare Klemmenleiste wieder einzusetzen.

1. Setzen Sie das Ende der abnehmbaren Klemmenleiste gegenüber dem Griff in die Basiseinheit ein. Beachten Sie, dass dieses Ende über einen gekrümmten Bereich verfügt, der im Montagesockel einrastet.



Haken Sie das Ende der abnehmbaren Klemmenleiste am Ende des Montagesockels ein, und drehen Sie es, bis es einrastet.

2. Drehen Sie die Klemmenleiste in den Montagesockel, bis diese an ihrer Position einrastet.

3. Wenn ein E/A-Modul installiert ist, lassen Sie den Hebel der abnehmbaren Klemmenleiste am Modul einrasten.

Ausbauen eines Montagesockels

Wenn Sie einen Montagesockel ausbauen möchten, müssen Sie alle installierten Module und das rechts neben dem Sockel installierte Modul ausbauen. Wenn der Montagesockel über eine abnehmbare Klemmenleiste verfügt, entriegeln Sie den Griff der abnehmbaren Klemmenleiste am E/A-Modul, und ziehen Sie am Griff, um die abnehmbare Klemmenleiste herauszuziehen.

WARNUNG

Wenn Sie das Modul bei aktivierter Backplane einsetzen oder entfernen, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Vergewissern Sie sich, bevor Sie fortfahren, dass die Spannungsversorgung getrennt wurde oder dass es sich um einen nicht explosionsgefährdeten Standort handelt.

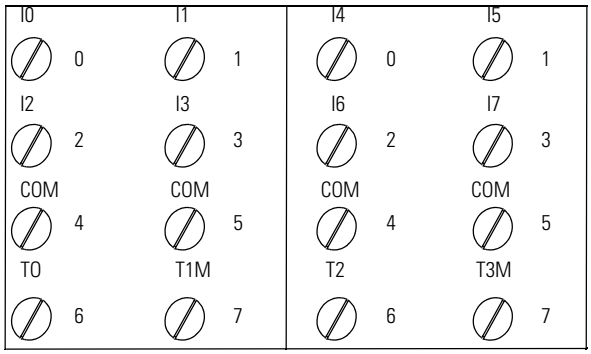
1. Ziehen Sie das E/A-Modul nach oben, um es aus dem Sockel zu entfernen.
2. Entfernen Sie das Modul rechts neben dem auszubauenden Sockel. Dies ist erforderlich, weil sich das Verriegelungsteil des Sockels unter dem benachbarten Modul befindet.
3. Verwenden Sie einen Schraubendreher, um die orangefarbene Halteschraube der DIN-Schiene am Montagesockel in die vertikale Position zu bringen. Auf diese Weise wird der Verriegelungsmechanismus gelöst.
4. Heben Sie den Montagesockel an, und entfernen Sie ihn von der DIN-Schiene.

Verdrahten der Module

Befolgen Sie beim Verdrahten der Module folgende Richtlinien:

- Verlegen Sie keine Kommunikations-, Eingangs- oder Ausgangsleitungen in Kabelkanälen, in denen sich Hochspannungsleitungen befinden. Siehe auch die Publikation 1770-4.1, Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen.
- Es wird empfohlen, die Verdrahtung ordnungsgemäß und unter Beachtung der Signalnamen aller Klemmen vorzunehmen.
- Ziehen Sie die Schrauben für Kommunikations- und E/A-Anschlüsse ordnungsgemäß fest.

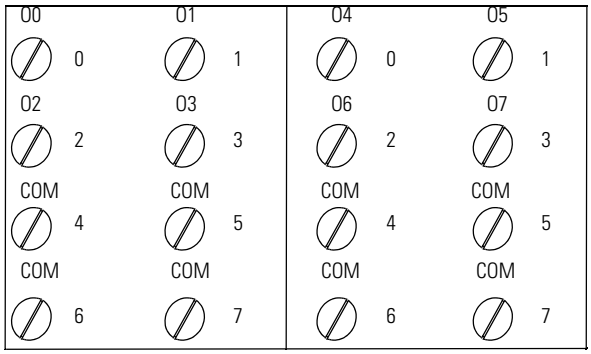
1734-IB8S-Feldanschlüsse



Die Abbildung zeigt die Sockel 1734-TOP und 1734-TB

Dabei gilt:
T0 = Testausgang 0
T1M = Testausgang 1 mit Muting
T2 = Testausgang 2
T3M = Testausgang 3 mit Muting
I0–I7 = Eingänge 0–7

1734-OB8S-Feldanschlüsse



Die Abbildung zeigt die Sockel 1734-TOP und 1734-TB

Dabei gilt:
O0–O7 = Sicherheitsausgänge 0–7
COM = Bezugspotenzial Netzteil

Festlegen der Netzknotenadresse eines POINT Guard I/O-Moduls

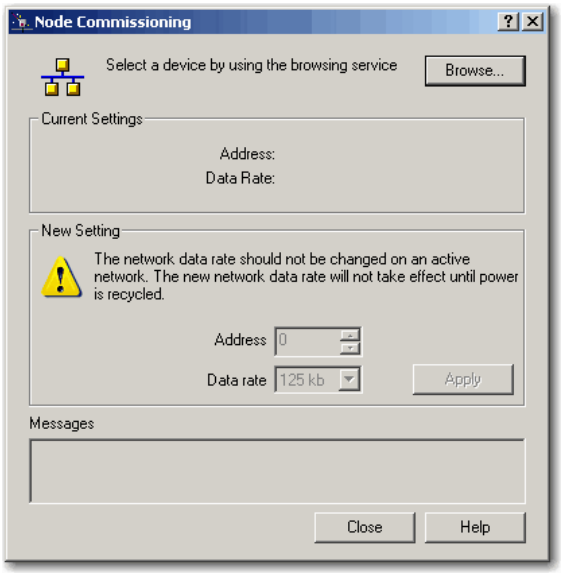
Legen Sie mithilfe der RSNetWorx for DeviceNet-Software die Netzknotenadresse von POINT Guard I/O-Modulen fest. Die ab Werk eingestellte Netzknotenadresse des Moduls lautet 63. Es wird empfohlen, die Module nacheinander anzuschließen und zu konfigurieren. Anderenfalls verhindern Adressenkonflikte (alle Module weisen die Netzknotenadresse 63 auf) die Kommunikation mit einigen Modulen.

WICHTIG

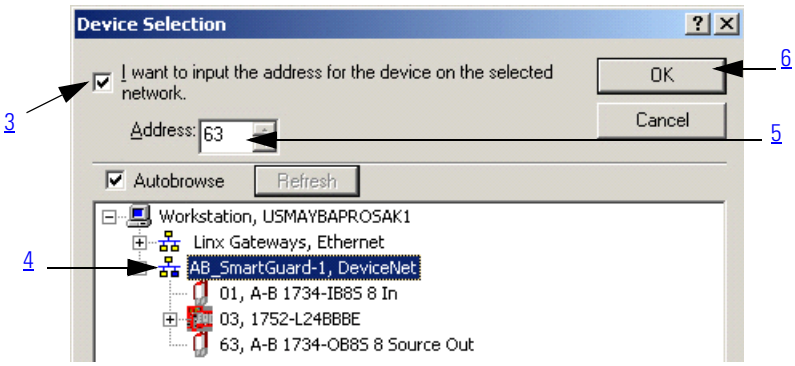
Die eindeutige Kennung für einen Sicherheitsknoten ist eine Kombination aus der Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse. Wenn die SNN festgelegt ist, wird die aktuelle Netzknotenadresse zum Generieren und Speichern dieser Kennung im Flash-Speicher verwendet. Sobald die Kennung festgelegt ist, kann die Netzknotenadresse aus Sicherheitsgründen nur noch geändert werden, wenn zum Zurücksetzen der Netzknotenadresse des POINT Guard I/O-Moduls besondere Maßnahmen ergriffen werden. **Aus diesem Grund müssen Sie die Netzknotenadresse vor dem Anwenden einer SNN festlegen.**

Gehen Sie wie folgt vor, um die Netzknotenadresse mit dem Tool zur Netzknoteninbetriebnahme festzulegen.

1. Wählen Sie Start>Programs (Programme)>Rockwell Software>RSNetWorx>DeviceNet Node Commissioning Tool aus.



2. Klicken Sie auf „Browse“ (Durchsuchen).



3. Aktivieren Sie das Feld „I want to input the address for the device on the selected network“ (Adresse für das Gerät im ausgewählten Netzwerk eingeben).

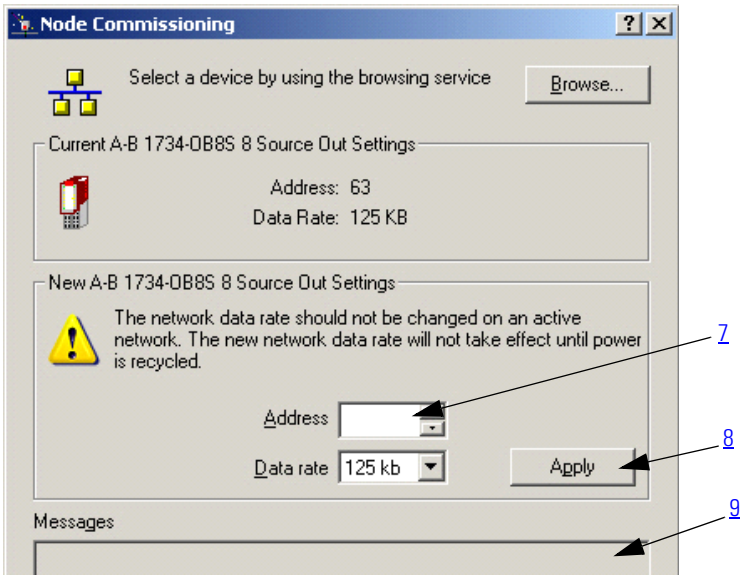
4. Durchsuchen Sie das DeviceNet-Netzwerk. Klicken Sie **nicht** auf OK, wenn der Suchvorgang abgeschlossen ist.

   Wenn Sie das DeviceNet-Netzwerk nicht durchsuchen können, die POINT Guard-Module dennoch angezeigt werden, wurden die Module eventuell bereits zuvor mit einer inkompatiblen Datenrate oder Netzknotenadresse konfiguriert. Versuchen Sie, diese Module einem separaten Netzwerk hinzuzufügen, um ihre Netzknotenadresse und Datenrate zu bestimmen.

5. Geben Sie die aktuelle Adresse für das Gerät ein.

   Die werkseitig eingestellte Netzknotenadresse lautet 63.

6. Klicken Sie auf OK.



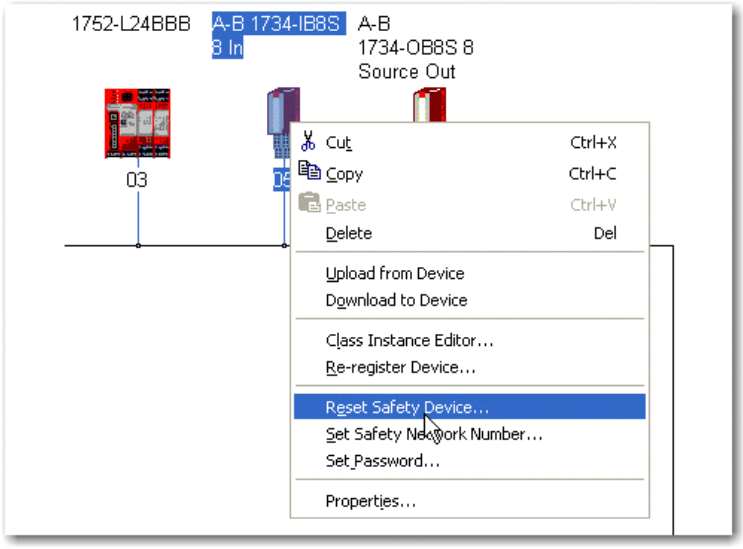
7. Geben Sie die neue Adresse für das Gerät ein.
8. Klicken Sie auf „Apply“ (Übernehmen).
9. Überprüfen Sie im Nachrichtenabschnitt, ob die Adresse bestätigt wird.

Zurücksetzen der POINT Guard I/O-Module auf die Werkseinstellungen

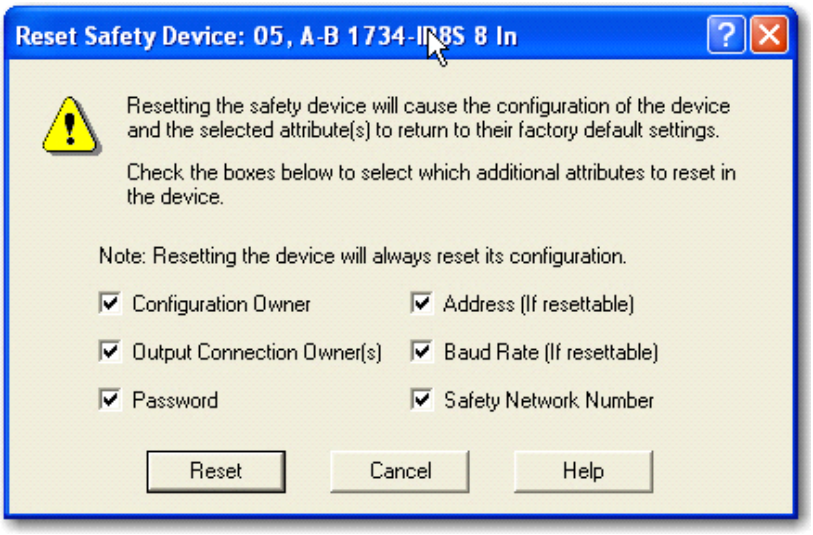
Eventuell ist es sinnvoll, Ihr POINT Guard I/O-Modul auf die Werkseinstellungen zurückzusetzen, bevor Sie die Netzknotenadresse der Module im DeviceNet-Netzwerk mit dem Tool zur Netzknoteninbetriebnahme festlegen. Wenn Ihr POINT Guard I/O-Modul beispielsweise zuvor einer verwaltenden Steuerung mit einer Sicherheitsverbindung zugewiesen war, kann das Modul erst dann eine Sicherheitsverbindung zu einer neuen verwaltenden Steuerung aufbauen, wenn die vorherige verwaltende Steuerung durch Zurücksetzen des Moduls gelöscht wurde. Verwenden Sie dazu die Software RSNetWorx for DeviceNet.

Gehen Sie wie folgt vor, um das Modul auf die Werkseinstellungen zurückzusetzen.

1. Klicken Sie mit der rechten Maustaste auf das Modul, und wählen Sie „Reset Safety Device“ (Sicherheitsgerät zurücksetzen) aus.



2. Aktivieren Sie alle Optionen.



3. Klicken Sie auf „Reset“ (Zurücksetzen).

Automatische Adressierung mit einem 1734-PDN-Adapter und mit POINT Guard I/O-Modulen

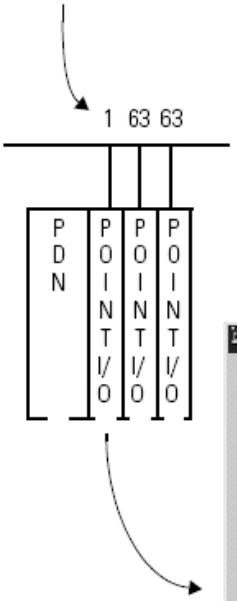
Bei der fortlaufenden automatischen Adressierung wird die Netzknotenadresse ganz links konfiguriert und ein Parameter in dem Modul festgelegt, das automatisch Netzknoten rechts vom Modul adressiert. Der Netzknoten ganz links kann ein POINT Guard I/O-Modul oder ein POINT I/O-Standardmodul sein.

Gehen Sie wie folgt vor, um die automatische Adressierung zu verwenden:

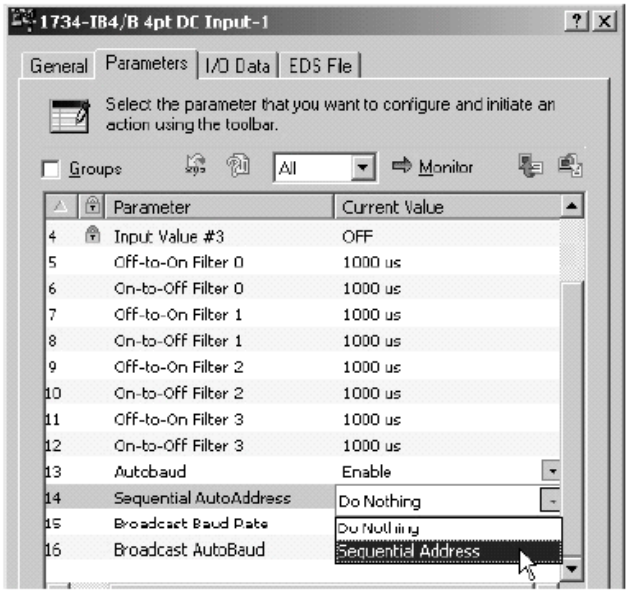
1. Setzen Sie alle Module zurück, von denen Sie nicht sicher sind, ob sie die Werkseinstellungen aufweisen oder nicht.
2. Schließen Sie das erste Modul am 1734-PDN-Adapter an.
3. Legen Sie die Netzknotenadresse dieses Moduls mit dem Tool zur Netzknoteninbetriebnahme fest.
4. Schließen Sie die zusätzlichen Module rechts von dem in Schritt 2 und 3 verwendeten Modul an.

5. Führen Sie die automatische Adressierungsfunktion für das in den Schritten 2 und 3 verwendete Modul aus.

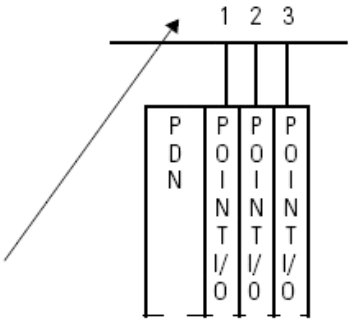
A. Legen Sie die Adresse des E/A-Moduls ganz links fest.



B. Wenn Sie das Modul ganz links konfigurieren, setzen Sie den Parameter „Sequential AutoAddress“ (Fortlaufende automatische Adressierung) auf „Sequential Address“ (Fortlaufende Adresse).



Das Modul setzt die Adressierung der übrigen Module in der Gruppe rechts von ihm fort.



Verdrahtung des Moduls

Thema	Seite
Einleitung	59
Verbindungsdetails	59
Beispiele für Verdrahtungen	61

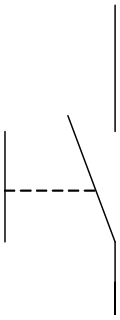
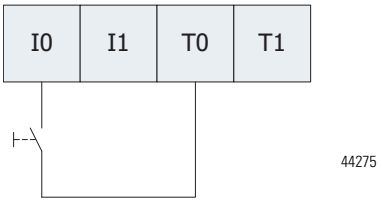
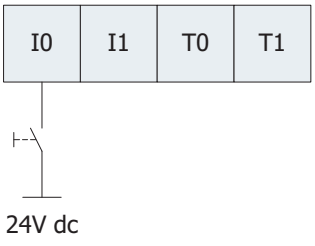
Einleitung

Dieses Kapitel enthält Informationen zur Verdrahtung und zu den Sicherheitskategorien.

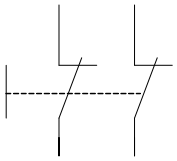
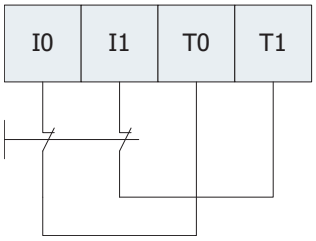
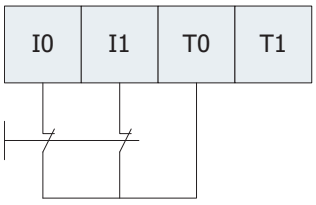
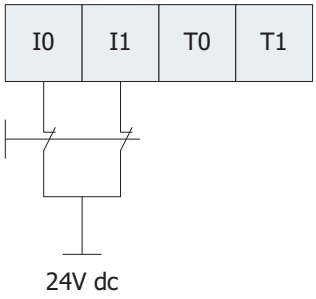
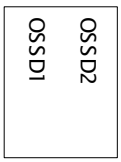
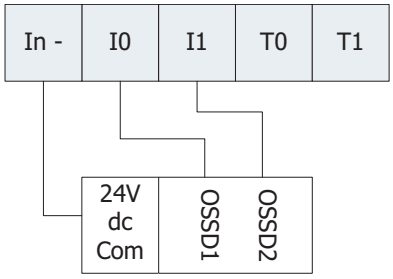
Verbindungsdetails

In den Tabellen sind die Anschlussmethoden für Eingangsgeräte und deren Sicherheitskategorien aufgeführt.

Angeschlossene Geräte und Sicherheitskategorien

Angeschlossenes Gerät	Testimpuls von Testausgang	Verbindung	Schematische Darstellung	Sicherheits-kategorie
Drucktaste 	Ja	Schließen Sie die Drucktaste zwischen I0 und T0 an. T0 muss als Testimpuls konfiguriert sein.		2
	Nein	Schließen Sie die Drucktaste zwischen 24 V DC und I0 an.		1

Angeschlossene Geräte und Sicherheitskategorien

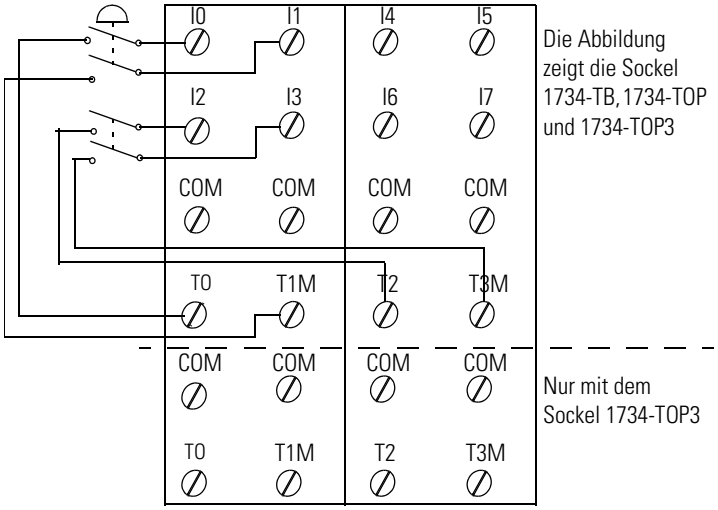
Angeschlossenes Gerät	Testimpuls von Testausgang	Verbindung	Schematische Darstellung	Sicherheits-kategorie
Not-Halt-Tasten Türüberwachungs-schalter 	Ja	Schließen Sie das Gerät zwischen I0 und T0 sowie zwischen I1 und T1 an.		4
	Nein	Schließen Sie das Gerät zwischen T0 und I0 und I1 an. Beachten Sie, dass T0 für ein 24-V-Netzteil konfiguriert ist.		3
		Schließen Sie die Geräte zwischen 24 V DC sowie I0 und I1 an.		
Lichtgitter 	Ja	Schließen Sie OSSD1 und OSSD2 an I0 und I1 an. Schließen Sie die Bezugspotenziale des 24-V-Netzteils an.		3 oder 4, abhängig vom verwendeten Lichtgitter

Beispiele für Verdrahtungen

Dieser Abschnitt enthält Beispiele für die anwendungsabhängige Verdrahtung. Das entsprechende Modul finden Sie über die Bestellnummern.

Zweikanalige Not-Halt-Geräte

Dieses Beispiel veranschaulicht die Verdrahtung und die Steuerungskonfiguration, wenn ein POINT Guard I/O-Modul mit einem Not-Halt-Tasten und einem Gate-Überwachungsschalter verwendet wird, die über zweikanalige Kontakte verfügen. Bei Verwendung in Kombination mit den Programmen in einer Sicherheitssteuerung entspricht diese Verdrahtung Sicherheitskategorie 4 (Not-Halt-Tasten) und Sicherheitskategorie 3 (Gate-Überwachungsschalter).



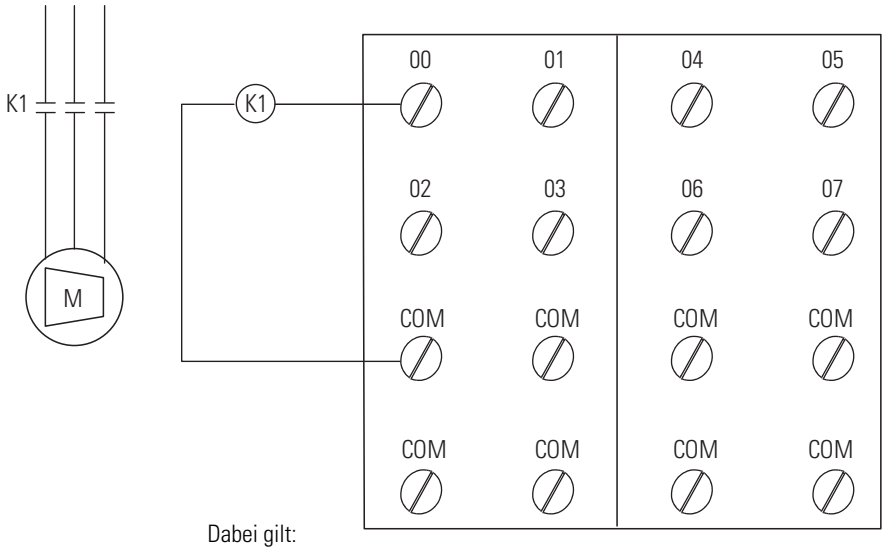
Steuerungs-konfiguration	Parametername	Konfigurationseinstellung
Sicherheits-eingang 0	Safety Input 0 Channel Mode (Kanalmodus Sicherheitseingang 0)	Test Pulse from Test Output (Impulstest von Testausgang)
	Safety Input 0 Test Source (Testquelle Sicherheitseingang 0)	Test Output 0 (Testausgang 0)
	Dual-channel Safety Input 0/1 Mode (Modus zweikanaliger Sicherheitseingang 0/1)	Dual-channel Equivalent (Zweikanalig gleichwertig)
	Dual-channel Safety Input 0/1 Discrepancy Time (Diskrepanzzeit zweikanaliger Sicherheitseingang 0/1)	100 ms (anwendungsabhängig)
Sicherheits-eingang 1	Safety Input 1 Channel Mode (Kanalmodus Sicherheitseingang 1)	Test Pulse from Test Output (Impulstest von Testausgang)
	Safety Input 1 Test Source (Testquelle Sicherheitseingang 1)	Test Output 1 (Testausgang 1)

Sicherheits-eingang 2	Safety Input 2 Channel Mode (Kanalmodus Sicherheitseingang 2)	Safety Input (Sicherheitseingang)
	Safety Input 2 Test Source (Testquelle Sicherheitseingang 2)	Test Output 2 (Testausgang 2)
	Dual-channel Safety Input 2/3 Mode (Modus zweikanaliger Sicherheitseingang 2/3)	Dual-channel Equivalent (Zweikanalig gleichwertig)
Sicherheits-eingang 3	Safety Input 3 Channel Mode (Kanalmodus Sicherheitseingang 3)	Safety Input (Sicherheitseingang)
	Safety Input 3 Test Source (Testquelle Sicherheitseingang 3)	Test Output 3 (Testausgang 3)
Testausgang 0	Test Output 0 Mode (Modus Testausgang 0)	Pulse Test Output (Impulstestausgang)
Testausgang 1	Test Output 1 Mode (Modus Testausgang 1)	Pulse Test Output (Impulstestausgang)
Testausgang 2	Test Output 2 Mode (Modus Testausgang 2)	Power Supply Output (Netzteilausgang)
Testausgang 3	Test Output 3 Mode (Modus Testausgang 3)	Power Supply Output (Netzteilausgang)

Einkanaliges Sicherheitsschütz

Das Beispiel zeigt die Verdrahtung und Steuerungskonfiguration bei Verwendung eines POINT Guard I/O-Moduls mit einem einkanaligen Sicherheitsschütz.

Bei Verwendung in Kombination mit den Programmen der Sicherheitssteuerung entspricht diese Schaltkreiskonfiguration der Sicherheitskategorie 2.



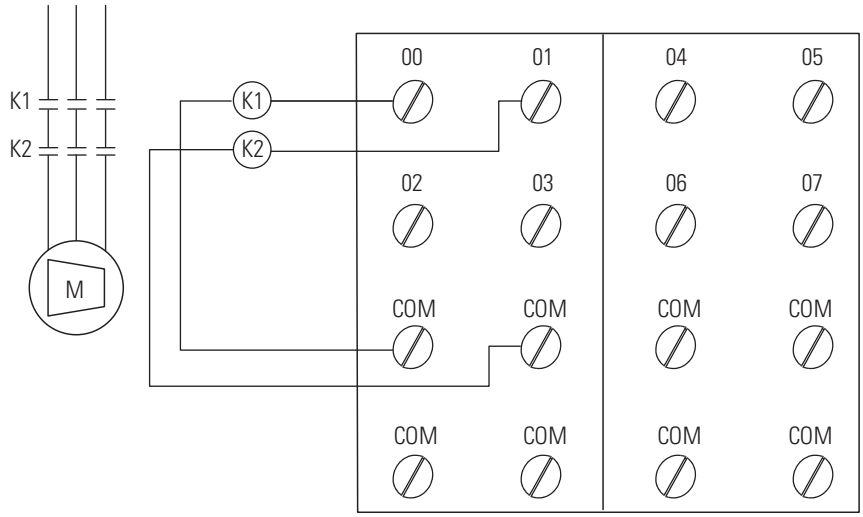
Dabei gilt:
00–07 = Sicherheitsausgänge
COM = Bezugspotenzial

Steuerungs-konfiguration	**Parametername**	**Konfigurationseinstellung**
Sicherheits-ausgang 0	Safety Output 0 Point Mode (Punktmodus Sicherheitsausgang 0)	Safety Pulse Test (Sicherheitsimpulstest)
	Point Operation – Type (Punktvorgang – Typ)	Single Channel (Einzelkanal)

Zweikanalige Sicherheitsschütze

Das Beispiel zeigt die Verdrahtung und Steuerungskonfiguration bei Verwendung eines POINT Guard I/O-Moduls mit redundanten Sicherheitsschützen.

Bei Verwendung in Kombination mit den Programmen der Sicherheitssteuerung entspricht diese Schaltkreiskonfiguration der Sicherheitskategorie 4. Eventuell ist eine zusätzliche Verdrahtung erforderlich, wie z. B. für die Überwachungsrückführung, um Sicherheitskategorie 4 zu erreichen.



Dabei gilt:
00–07 = Sicherheitsausgänge
COM = Bezugspotenzial

Steuerungs-konfiguration	Parametername	Konfigurationseinstellung
Sicherheits-ausgang 0	Safety Output 0 Point Mode (Punktmodus Sicherheitsausgang 0)	Safety Pulse Test (Sicherheitsimpulstest)
	Point Operation – Type (Punktvorgang – Typ)	Dual-channel (Zweikanalig)
Sicherheits-ausgang 1	Safety Output 1 Point Mode (Punktmodus Sicherheitsausgang 1)	Safety Pulse Test (Sicherheitsimpulstest)

Notizen:

Beispiele für Netzteile

Thema	Seite
Einleitung	67
POINTBus-Backplane	67
Beispiele für Netzteile	68
Vorsichtsmaßnahmen für die sichere Verwendung	71

Einleitung

Ein POINT Guard I/O-System besteht aus einem Adapter, E/A-Modulen, Montagesockeln und Stromversorgungsmodulen. POINT I/O-Adapter verfügen über integrierte Stromversorgungsmodule. Alle POINT I/O-Module werden über die POINTBus-Backplane gespeist – mittels Adapter oder Erweiterungsnetzteil.

POINTBus-Backplane

Die POINTBus-Backplane besteht aus einem 5-V-Kommunikations-Bus und einer Feldsammelschiene. Diese werden über den Adapter oder über Netzteile mit Spannung versorgt. Beim Auswählen der Netzteiltypen für Ihre Anforderungen **müssen** Sie beim Konzipieren einer POINTBus-Backplane den Stromverbrauch des 5-V- und 24-V-Busses berücksichtigen.

Für die POINTBus-Backplane und die Feldversorgung stehen folgende Netzteile zur Verfügung:

- Verwenden Sie das Erweiterungsnetzteil 1734-EP24DC mit dem 5-V- und/oder 24-V-Bus.
- Verwenden Sie das Erweiterungsnetzteil 1734-EPAC, um 120/240-V-AC-Feldstrom an die E/A-Module rechts daneben weiterzuleiten.

WICHTIG

Wenn Sie das 1734-EPAC-Erweiterungsnetzteil links neben den POINT Guard I/O-Modulen verwenden, benötigen Sie einen 1734-FPD-Feldstromverteiler oder ein 1734-EP24DC-Erweiterungsnetzteil, um die POINT Guard I/O-Feldversorgung von der AC-Feldversorgung zu trennen.

Zum Einrichten und Verwalten der Kommunikation (Verbindung) zwischen dem Modul und der Steuerung ist eine 5-V-POINTBus-Versorgung erforderlich.

- Die Netzteile 1734-EP24DC und 1734-EPAC stellen zwei Dienste zur Verfügung.
  - Trennung der Feldstromverteilung links vom Netzteil von der Feldstromverteilung rechts vom Netzteil.
  - Fügt zusätzliche 1,3 A des 5-V-Stroms zur POINTBus-Backplane für E/A-Module rechts vom Netzteil hinzu.
- Verwenden Sie den 1734-FPD-Feldstromverteiler mit dem 5-V-Bus. Der 1734-FPD-Feldstromverteiler leitet alle POINT I/O-Backplane-Signale weiter, einschließlich des 5-V-Busses auf der linken Seite. Er stellt jedoch keinen **zusätzlichen** POINTBus-Backplane-Strom zur Verfügung. Auf diese Weise können Sie Feldstromsegmente trennen.

Berücksichtigen Sie bei Verwendung der POINT Guard I/O-Module folgende Empfehlungen:

- Verwenden Sie mit den GuardLogix-Steuerungen den 1734-AENT-Adapter.
- Verwenden Sie mit der SmartGuard-Steuerung den 1734-PDN-Adapter.

Die Adapter und Netzteile unterscheiden sich hinsichtlich der Strommenge, die sie dem 5-V- und/oder 24-V-Bus zur Verfügung stellen.

Weitere Informationen finden Sie in der Publikation 1734-SG001, POINT I/O Selection Guide.

Beispiele für Netzteile

Anhand der folgenden gültigen Beispielkonfigurationen für Netzteile sollen die möglichen Netzteilkombinationen für Ihr System veranschaulicht werden:

- Beispiel 1: POINT Guard I/O mit 1734-EP24DC (Eingang), 1734-FPD (Ausgang) – Nur 24-V-DC-E/A auf Seite 69
- Beispiel 2: POINT Guard I/O mit 1734-EP24DC für Eingang und Ausgang, plus AC-E/A auf Seite 70

Diese Beispiele dienen lediglich zur Veranschaulichung der verschiedenen Spannungsversorgungskonzepte.

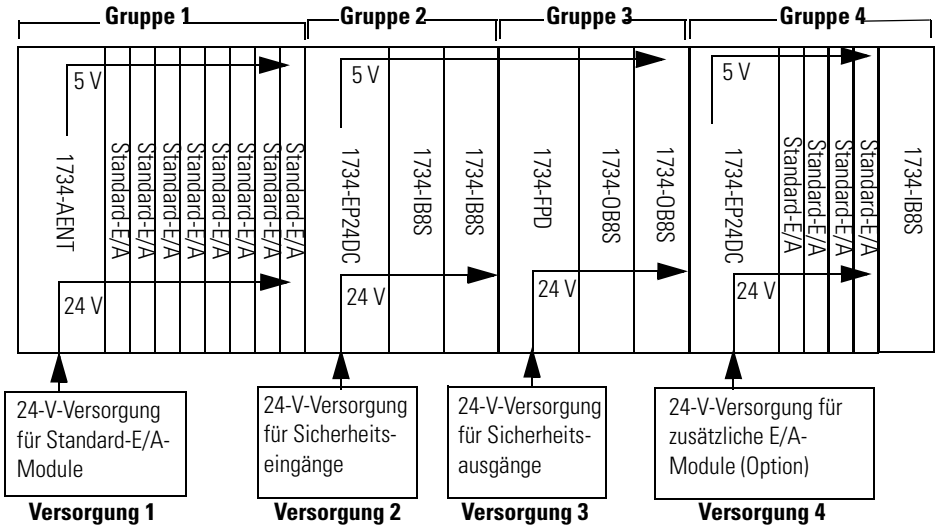
WICHTIG

- Sie müssen die Anforderungen für Ihre Anwendung definieren, um die Feld- und Zwischenkreisspannung zu trennen.
- Für POINT Guard I/O ist keine separate Feldzwischenkreispannung erforderlich. Es müssen also für die Module 1734-IB8S und 1734-OB8S keine separaten Netzteile verwendet werden. Dies ist optional.
- Für POINT Guard I/O ist kein separates POINTBus-Netzteil (Kommunikation) erforderlich, um eine Trennung von anderen POINT I/O-Modulen zu erzielen, es sei denn, es ist eine zusätzliche POINTBus-Versorgung erforderlich.

Beispiel 1: POINT Guard I/O mit 1734-EP24DC (Eingang), 1734-FPD (Ausgang) – Nur 24-V-DC-E/A

In diesem Netzteilbeispiel wird ein Erweiterungsnetzteil 1734-EP24DC und ein Feldstromverteiler 1734-FPD verwendet, um E/A mit folgenden Eigenschaften zu versorgen:

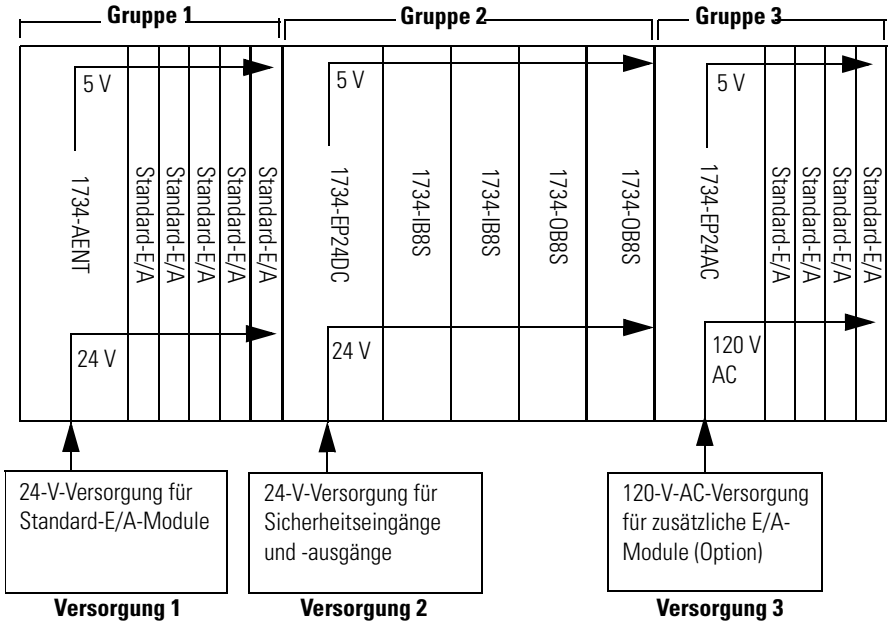
- E/A der Gruppe 1 und Gruppe 4 weisen im Vergleich zu den übrigen E/A separate E/A-Funktionsgruppen auf.
- Der Feldstrom für Gruppe 3 stammt von einem Netzteil, das von der Bus-Kommunikationsversorgung getrennt ist (der Ausfall von Versorgung 3 wird von der Steuerung erkannt).
- Der Feldstrom für Gruppe 2 befindet sich auf demselben Netzteil wie die Bus-Kommunikationsversorgung für Gruppe 2 und Gruppe 3 (der Ausfall von Versorgung 2 führt zu unterbrochenen Verbindungen zur Steuerung für die Gruppen 2 und 3).



Beispiel 2: POINT Guard I/O mit 1734-EP24DC für Eingang und Ausgang, plus AC-E/A

In diesem Netzteilbeispiel wird ein 1734-EP24DC-Eingang und -Ausgang mit diesen Eigenschaften verwendet:

- E/A der Gruppe 1 und Gruppe 3 weisen im Vergleich zu Gruppe 2 separate Funktionsgruppen auf.
- Der Feldstrom für Ausgänge der Gruppe 2 stammt vom selben Netzteil, das auch für die Bus-Kommunikation verantwortlich ist (der Ausfall von Versorgung 2 führt zu einer Unterbrechung der Verbindungen zur Steuerung).
- Der Feldstrom für Eingänge der Gruppe 2 stammt vom selben Netzteil, das auch für die Bus-Kommunikation verantwortlich ist (der Ausfall von Versorgung 2 führt zu einer Unterbrechung der Verbindungen zur Steuerung).



Vorsichtsmaßnahmen für die sichere Verwendung

Berücksichtigen Sie diese Richtlinien, um eine ordnungsgemäße Verwendung des Produkts zu gewährleisten:

- Schließen Sie an den POINT Guard I/O-Modulen keine AC-Spannung an.
- Bevor Sie das System, in dem das Modul integriert ist, in Betrieb nehmen, müssen Sie die Leiter ordnungsgemäß verdrahten und sicherstellen, dass das Modul funktioniert. Eine falsche Verdrahtung kann zum Verlust der Sicherheitsfunktion führen.
- Schließen Sie an den POINT Guard I/O-Modulen keine DC-Spannungen an, die über den Bemessungsspannungen liegen.
- Legen Sie an den Moduleingängen die richtigen Spannungen an. Das Anlegen falscher Spannungen kann zu Fehlfunktionen des Moduls führen, also den Verlust von Sicherheitsfunktionen und Beschädigungen des Moduls mit sich bringen.

Notizen:

Konfiguration des Moduls in einer GuardLogix-Steuerung

Thema	Seite
Einleitung	73
Verwenden der Hilfe	74
Hinzufügen von Modulen zum E/A-Konfigurationsbaum	74
Hinzufügen und Konfigurieren des Ethernet-Bridge-Moduls	74
Hinzufügen und Konfigurieren des 1734-AENT-Adapters	78
Hinzufügen und Konfigurieren von Sicherheitseingangsmodulen	82
Hinzufügen und Konfigurieren von Sicherheitsausgangsmodulen	88
Werte und Zustände von Tags	93
Konfigurieren der Registerkarte „Safety“ (Sicherheit)	94
Verwaltungsrechte für die Konfiguration	97
Konfigurationssignatur	97
Konfigurieren der Registerkarte „Input Configuration“ (Eingangskonfiguration)	98
Konfigurieren der Registerkarte „Input Configuration“ (Eingangskonfiguration)	98
Konfigurieren der Registerkarte „Test Output“ (Testausgang)	102
Konfigurieren der Registerkarte „Output Configuration“ (Ausgangskonfiguration)	103
Speichern und Herunterladen der Modulkonfiguration	105

Einleitung

Wenn Sie eine GuardLogix-Steuerung verwenden, konfigurieren Sie die POINT Guard I/O-Module mit der RSLogix 5000-Software, Version 17, indem Sie das entsprechende Add-On-Profil verwenden.

WICHTIG Sie **müssen** jeden Punkt konfigurieren, der als Sicherheitseingang oder -ausgang verwendet werden soll. Standardmäßig sind alle Sicherheitseingänge und -ausgänge deaktiviert.

TIPP Sie können ein Add-On-Profil über die RSLogix 5000-Support-Website unter http://support.rockwellautomation.com/ControlFlash/LogixProfiler.asp herunterladen.

Verwenden der Hilfe

Klicken Sie am unteren Rand eines Dialogfelds auf „Help“ (Hilfe), um Informationen zum Ausfüllen des jeweiligen Dialogfelds aufzurufen. Klicken Sie am unteren Rand eines Warnfensters auf „Help“ (Hilfe), um Informationen zum angezeigten Fehler aufzurufen.

Hinzufügen von Modulen zum E/A-Konfigurationsbaum

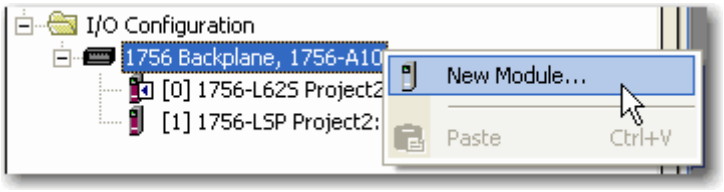
Wenn Sie Ihre POINT Guard I/O-Module erstmalig für den Einsatz mit der GuardLogix-Steuerung konfigurieren, befolgen Sie bei Bedarf die folgenden Schritte:

1. Hinzufügen und Konfigurieren des Ethernet-Bridge-Moduls.
2. Hinzufügen und Konfigurieren des 1734-AENT-Adapters.
3. Hinzufügen und Konfigurieren von Sicherheitseingangsmodulen.
4. Hinzufügen und Konfigurieren von Sicherheitsausgangsmodulen.

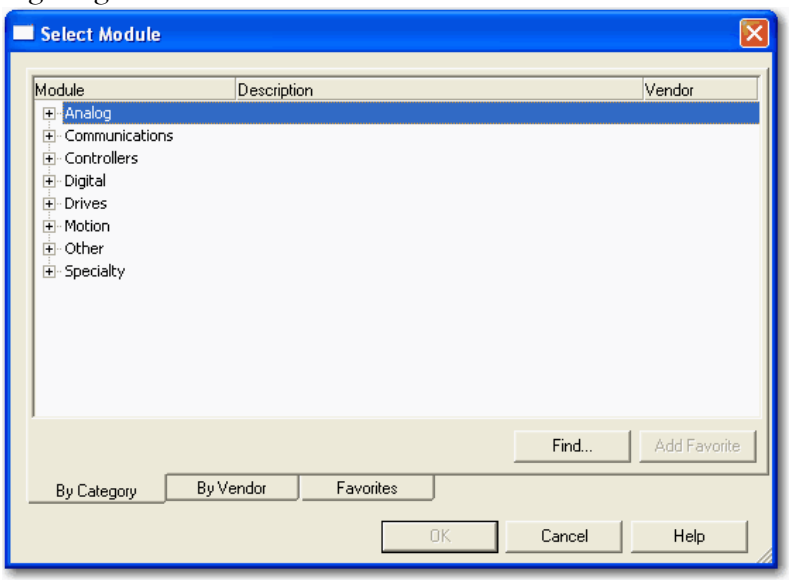
Hinzufügen und Konfigurieren des Ethernet-Bridge-Moduls

Gehen Sie zum Hinzufügen und Konfigurieren des Ethernet-Bridge-Moduls wie folgt vor:

1. Klicken Sie im E/A-Konfigurationsbaum mit der rechten Maustaste auf „1756 Backplane, 1756-A*xx*“, und wählen Sie die Option „New Module“ (Neues Modul) aus.



Das Dialogfeld „Select Module“ (Modul auswählen) wird angezeigt.



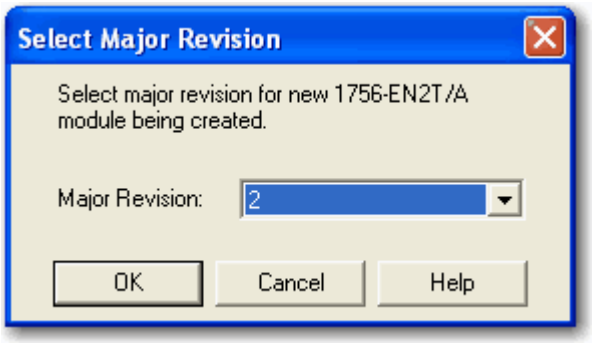
2. Erweitern Sie die Option „Communications“ (Kommunikation), wählen Sie eines der folgenden Ethernet-Bridge-Module aus, und klicken Sie auf OK.

Bestellnummer	Beschreibung
1756-EN2F/A	1756 10/100 Mbit/s Ethernet-Bridge, LWL-Medien
1756-EN2T/A	1756 10/100 Mbit/s Ethernet-Bridge, verdrillte Doppelmedien
1756-ENBT/A	1756 10/100 Mbit/s Ethernet-Bridge, verdrillte Doppelmedien

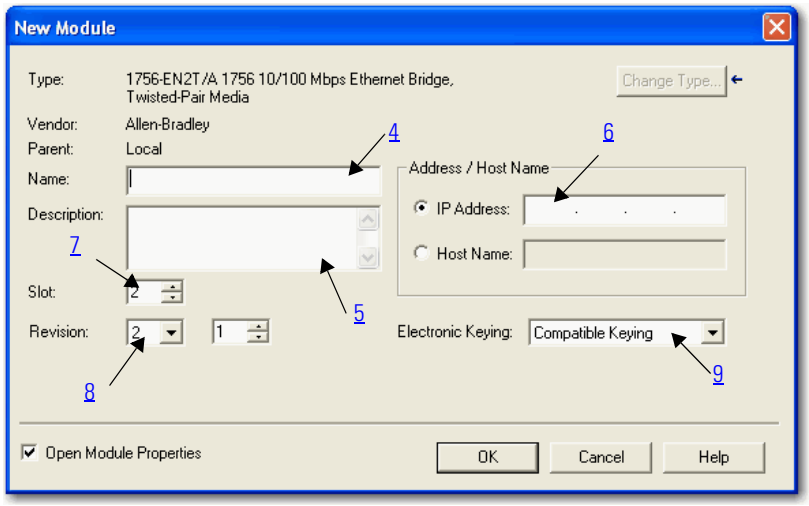
Für dieses Beispiel wurde das Bridge-Modul 1756-EN2T/A ausgewählt.

3. Geben Sie die Nummer der Hauptversion des Bridge-Moduls ein, und klicken Sie auf OK.

Bestellnummer	Kompatible Hauptversion
1756-EN2F/A	1 oder höher
1756-EN2T/A	1 oder höher
1756-ENBT/A	3 oder höher



Das Dialogfenster „New Module“ (Neues Modul) wird angezeigt.



4. Geben Sie in das Feld „Name“ den entsprechenden Namen des Ethernet-Bridge-Moduls ein.

5. Geben Sie in das Feld „Description“ (Beschreibung) eine optionale Beschreibung des Ethernet-Bridge-Moduls ein.

6. Geben Sie in das Feld „IP Address“ (IP-Adresse) die entsprechende IP-Adresse des Ethernet-Bridge-Moduls ein.

7. Geben Sie in das Feld „Slot“ (Steckplatz) die entsprechende Steckplatznummer des Ethernet-Bridge-Moduls ein.

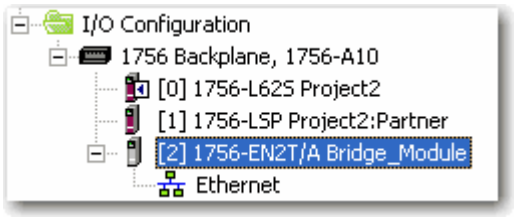
8. Geben Sie in die Felder „Revision“ (Version) die entsprechende Haupt- und Nebenversion des Bridge-Moduls ein.

9. Wählen Sie im Pulldown-Menü „Electronic Keying“ (Elektronische Codierung) die gewünschte Codierungsmethode für das Ethernet-Bridge-Modul aus.

Auswahl	Beschreibung
Compatible Module (Kompatibles Modul)	Mit dieser Option kann ein Modul feststellen, ob es das Modul, das in der von der Steuerung gesendeten Konfiguration definiert ist, emulieren kann.
Disable Keying (Codierung deaktivieren)	Die Parameter im physischen Modul und im in der Software konfigurierten Modul müssen nicht übereinstimmen. **Wählen Sie „Disable Keying“ (Codierung deaktivieren) nicht aus.**
Exact Match (Exakte Übereinstimmung)	Alle Parameter müssen übereinstimmen, da anderenfalls das eingesetzte Modul eine Verbindung zur Steuerung zurückweist.

10. Klicken Sie auf OK.

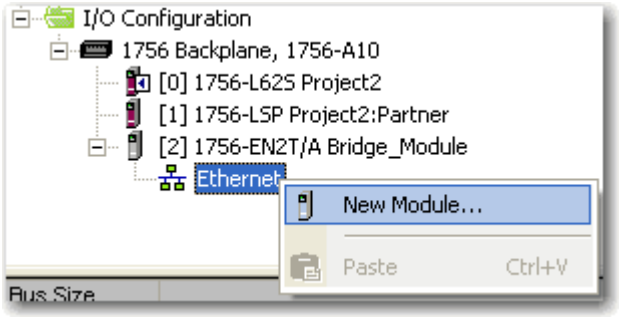
Im E/A-Konfigurationsbaum wird die Ethernet-Verbindung angezeigt.



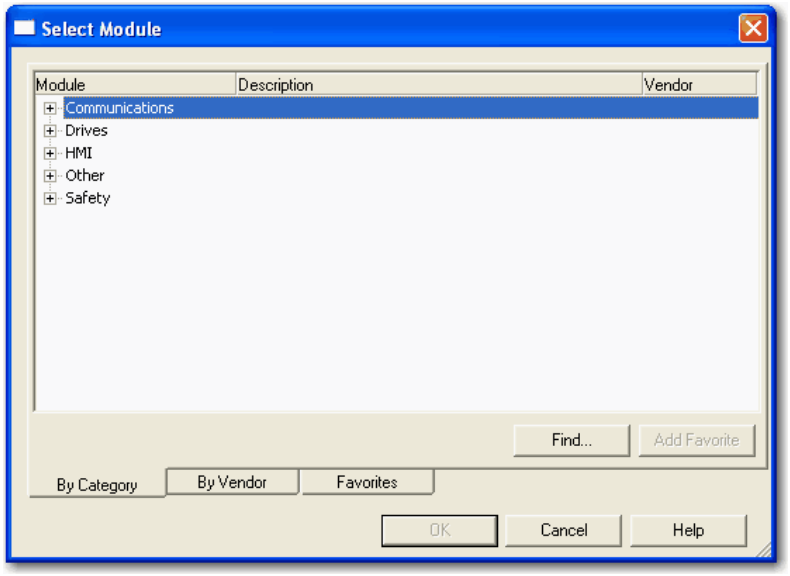
Hinzufügen und Konfigurieren des 1734-AENT-Adapters

Gehen Sie wie folgt vor, um den 1734-AENT-Adapter zu konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf die Ethernet-Verbindung, und wählen Sie „New Module“ (Neues Modul) aus.

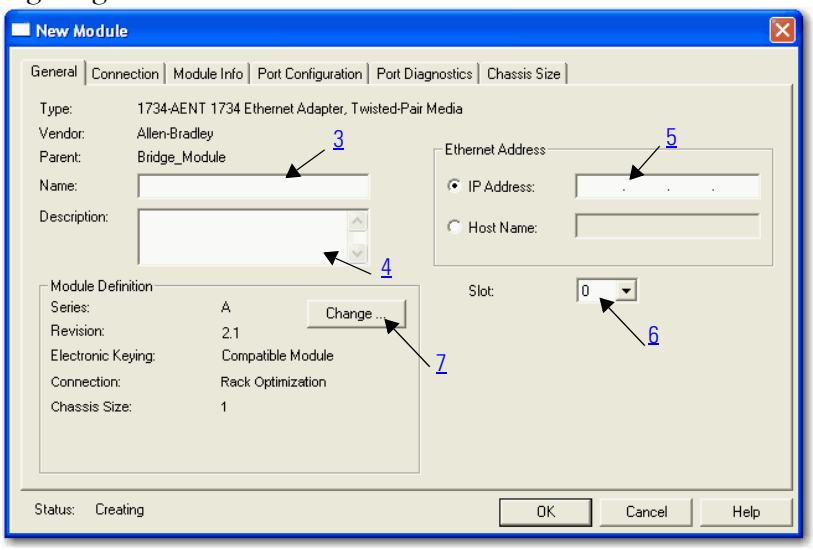


Das Dialogfeld „Select Module“ (Modul auswählen) wird angezeigt.



2. Erweitern Sie den Knoten „Communications“ (Kommunikation), und wählen Sie den 1734-AENT-Adapter aus.

Das folgende Dialogfenster „New Module“ (Neues Modul) wird angezeigt.



3. Geben Sie in das Feld „Name“ den entsprechenden Namen des 1734-AENT-Adapters ein.

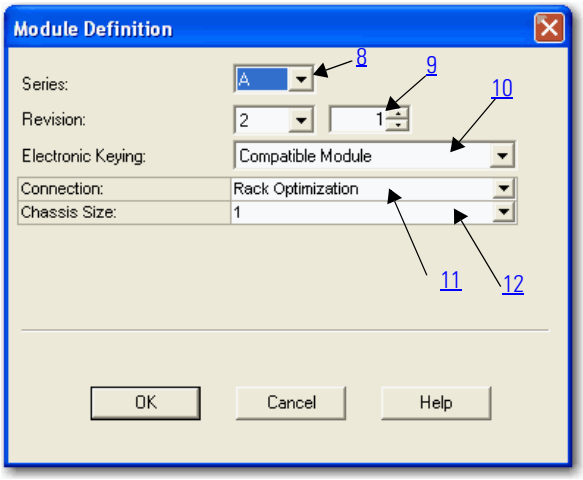
4. Geben Sie in das Feld „Description“ (Beschreibung) eine optionale Beschreibung des 1734-AENT-Adapters ein.

5. Geben Sie in das Feld „IP Address“ (IP-Adresse) die entsprechende IP-Adresse des 1734-AENT-Adapters ein.

6. Geben Sie in das Feld „Slot“ (Steckplatz) die entsprechende Steckplatznummer des 1734-AENT-Adapters ein.

7. Klicken Sie im Bereich „Module Definition“ (Moduldefinition) auf „Change“ (Ändern).

   Das Dialogfeld „Module Definition“ (Moduldefinition) wird angezeigt.



8. Geben Sie in das Feld „Series“ (Serie) den entsprechenden Serienbuchstaben des 1734-AENT-Adapters ein.

9. Geben Sie in die Felder „Revision“ (Version) die entsprechende Haupt- und Nebenversion des 1734-AENT-Adapters ein.

WICHTIG Zur Unterstützung von POINT Guard I/O-Modulen muss als 1734-AENT-Adapterfirmware Hauptversion 3 oder höher verwendet werden.

10. Wählen Sie im Pulldown-Menü „Electronic Keying“ (Elektronische Codierung) die gewünschte Codierungsmethode für den 1734-AENT-Adapter aus.

Auswahl	Beschreibung
Exact Match (Exakte Übereinstimmung)	Modul- und Typenserie müssen exakt übereinstimmen, da anderenfalls das Modul von der Steuerung zurückgewiesen wird.
Compatible Module (Kompatibles Modul)	Die Steuerung überprüft den Modultyp und die Version auf Kompatibilität. Kompatible Module, die übereinstimmen oder neuer sind, werden akzeptiert.
Disable Keying (Codierung deaktivieren)	Die Steuerung überprüft den Modultyp, akzeptiert jedoch jede Version. **Wählen Sie „Disable Keying“ (Codierung deaktivieren) nicht aus.**

11. Wählen Sie im Pulldown-Menü „Connection“ (Verbindung) die entsprechende Verbindung für den 1734-AENT-Adapter aus.

Auswahl	Beschreibung
Listen Only (Nur Hören)	Digitale E/A-Standarddaten werden gelesen oder verifiziert, die Module werden jedoch nicht gesteuert. (Wenn Sie mit mehreren Steuerungen arbeiten, dient eine Steuerung zum Steuern und die anderen Steuerungen zur Überwachung.)
None (Keine)	Der Adapter stellt eine direkte Verbindung zu allen Modulen her, die im E/A-Konfigurationsbaum unter dem 1734-AENT-Adapter aufgeführt sind.
Rack-Optimierung	Die digitalen E/A-Standarddaten werden in einem einzigen Rack-Image erfasst. **Dabei werden Sonder-, Analog- oder POINT Guard I/O-Module nicht berücksichtigt.**

TIPP Wenn Sie in Ihrem POINT I/O-System keine digitalen E/A-Standardmodule verwenden, wählen Sie „None“ (Keine) aus.

12. Wählen Sie im Pulldown-Menü „Chassis Size“ (Chassisgröße) die Anzahl der POINT I/O-Module aus, die am 1734-AENT-Adapter angeschlossen werden sollen, plus 1 für den 1734-AENT-Adapter.

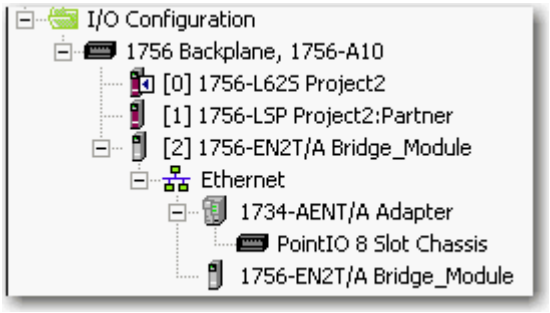
WICHTIG Die Klemmeneinheiten werden nicht gezählt. Geben Sie nur die Anzahl der installierten physischen Module ein, plus 1 für den Adapter. Die Zahl muss exakt mit der tatsächlichen Anzahl übereinstimmen. Sie können keine höhere Zahl für eventuelle spätere Erweiterungen eingeben.

13. Klicken Sie auf OK.

Sie kehren in das Dialogfeld „Module Properties“ (Moduleigenschaften) zurück.

14. Klicken Sie auf OK, um Ihre Änderungen anzuwenden.

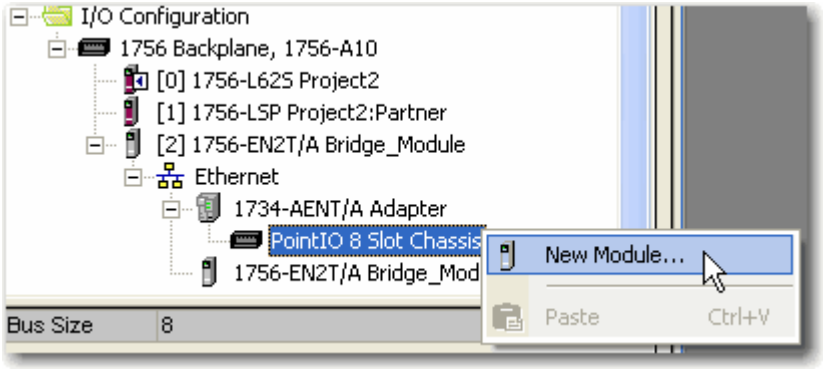
Im E/A-Konfigurationsbaum wird der 1734-AENT-Adapter angezeigt.



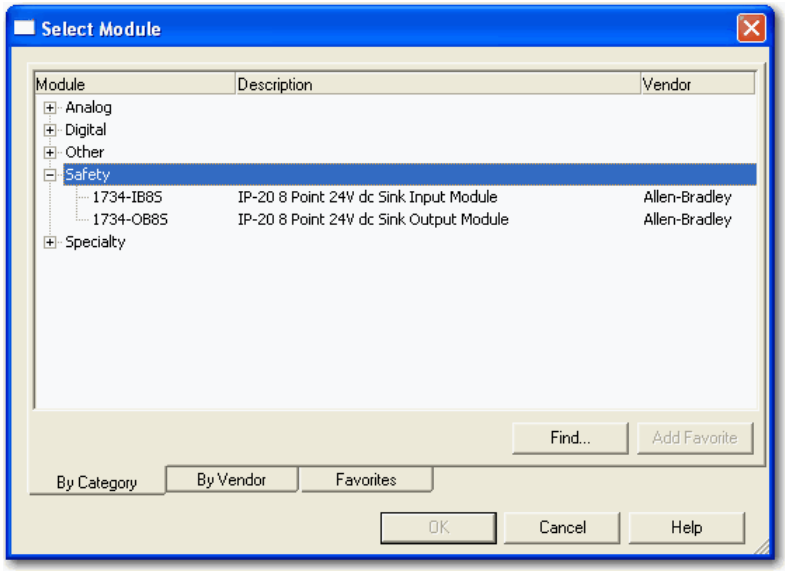
Hinzufügen und Konfigurieren von Sicherheitseingangsmodulen

Gehen Sie wie folgt vor, um POINT Guard I/O-Sicherheitsmodule hinzuzufügen und zu konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf das POINT I/O-Chassis, und wählen Sie „New Module“ (Neues Modul) aus.

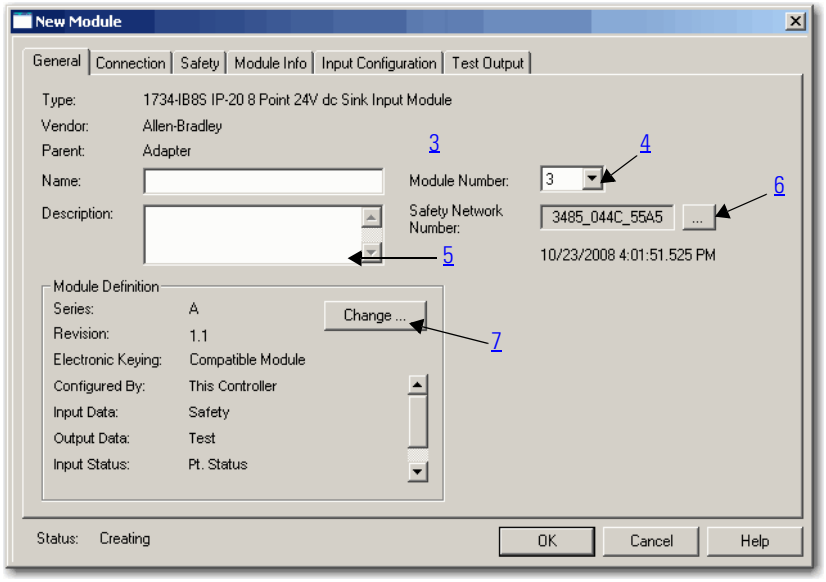


   Das Dialogfeld „Select Module“ (Modul auswählen) wird mit einer Liste angezeigt, die u. a. den Punkt „Safety“ (Sicherheit) enthält.



2. Wählen Sie das gewünschte Eingangsmodul aus, z. B. 1734-IB8S, und klicken Sie auf OK.

Das Dialogfeld „New Module“ (Neues Modul) wird angezeigt.



3. Geben Sie in das Feld „Name“ einen eindeutigen Namen für das Eingangsmodul ein.

4. Geben Sie in das Feld „Module Number“ (Modulnummer) eine eindeutige Modulnummer für das Eingangsmodul ein.

5. Geben Sie in das Feld „Description“ (Beschreibung) eine Beschreibung des Eingangsmoduls ein, wenn Sie dies wünschen.

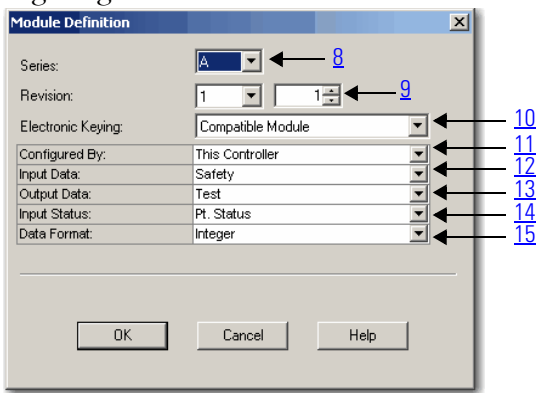
6. Verwenden Sie im Feld „Safety Network Number“ (Sicherheitsnetzwerknummer) die Standardeinstellung.

   Eine ausführliche Erläuterung der Sicherheitsnetzwerknummer (SNN) finden Sie in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch. In den meisten Fällen verwenden Sie die von der Software RSLogix 5000 vorgeschlagene Standardeinstellung.

   Mit der Sicherheitsnetzwerknummer (SNN) soll sichergestellt werden, dass jedes Modul in einem System eindeutig identifiziert werden kann. Es wird empfohlen, allen Sicherheitsmodulen in einem Netzwerk dieselbe SNN zuzuordnen, um die Dokumentation zu vereinfachen. Während der Konfiguration ordnet die Software RSLogix 5000 einem Sicherheitsgerät standardmäßig die Sicherheitsnetzwerknummer zu, die dem niedrigsten Sicherheitsknoten im Netzwerk entspricht.

7. Klicken Sie auf „Change“ (Ändern), um die Moduldefinition zu bearbeiten.

   Das Dialogfeld „Module Definition“ (Moduldefinition) wird angezeigt.



8. Geben Sie in das Feld „Series“ (Serie) den Serienbuchstaben des Eingangsmoduls ein.

9. Geben Sie in die Felder „Revision“ (Version) die Versionsnummern des Eingangsmoduls ein.

10. Wählen Sie im Pulldown-Menü „Electronic Keying“ (Elektronische Codierung) die gewünschte Codierungsmethode für das Eingangsmodul aus.

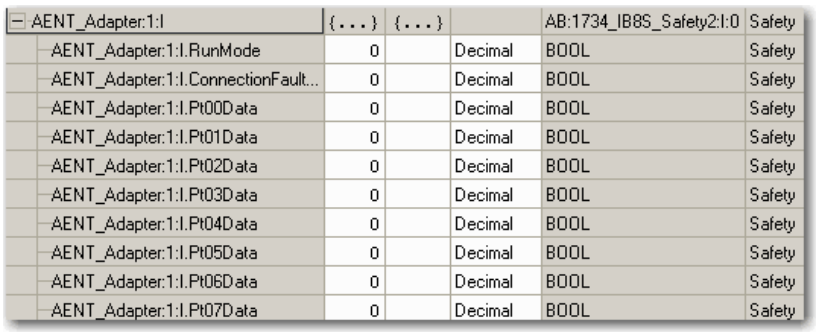
Auswahl	Beschreibung
Exact Match (Exakte Übereinstimmung)	Alle Parameter müssen übereinstimmen, da anderenfalls das eingesetzte Modul eine Verbindung zur Steuerung zurückweist.
Compatible Module (Kompatibles Modul)	Mit dieser Option kann ein E/A-Modul feststellen, ob es das Modul, das in der von der Steuerung gesendeten Konfiguration definiert ist, emulieren kann.

11. Wählen Sie im Pulldown-Menü „Configured By“ (Konfiguriert von) die gewünschte Konfigurationsmethode für dieses Modul aus.

Auswahl	Beschreibung
This Controller (Diese Steuerung)	Mit dieser Auswahl wird die Steuerung angewiesen, die Eingänge und Testausgänge zu konfigurieren.
External Means (Externe Mittel)	Mit dieser Auswahl wird die Steuerung angewiesen, ausschließlich eine Sicherheitseingangsverbindung herzustellen. Die Steuerung konfiguriert das Modul nicht und steuert auch die Testausgänge nicht.

12. Wählen Sie im Pulldown-Menü „Input Data“ (Eingangsdaten) die gewünschte Methode für das Eingangsmodul aus: „Safety“ (Sicherheit) oder „None“ (Keine).

Auswahl	Beschreibung
Sicherheit	Diese Tags werden für das Zielmodul erstellt: • RunMode für den Modulmodus • ConnectionFaulted für den Kommunikationsstatus • Safety Data für Sicherheitseingänge vom Modul

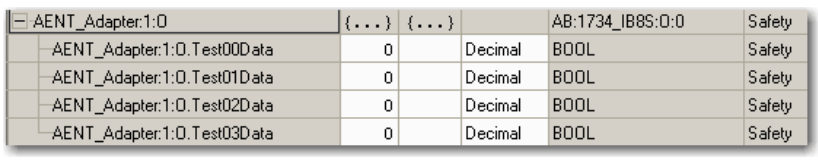


AENT_Adapter:1:I	{...}	{...}		AB:1734_IB8S_Safety2:I:0	Safety
AENT_Adapter:1:I.RunMode	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.ConnectionFault...	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt00Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt01Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt02Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt03Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt04Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt05Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt06Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt07Data	0		Decimal	BOOL	Safety

13. Wählen Sie im Pulldown-Menü „Output Data“ (Ausgangsdaten) die entsprechende Methode aus den folgenden Optionen aus.

WICHTIG Die Testausgänge, die als Standardausgänge am Modul konfiguriert sind, dürfen nicht zu Sicherheitszwecken verwendet werden.

Auswahl	Beschreibung
None (Keine)	Führt zu einer ausschließlichen Eingangsverbindung zum Modul. Eingänge und Status werden gelesen, doch es werden keine Ausgänge geschrieben. Sie können die Testausgänge weiterhin als Impulstestausgänge oder als Netzteil verwenden.
Test[a]	Erstellt diese Tags, um die Netzwerksteuerung der Testausgänge am Modul zu aktivieren. Diese Auswahl ermöglicht die Verwendung der Testausgänge als Standardausgänge und Muting-Ausgänge.

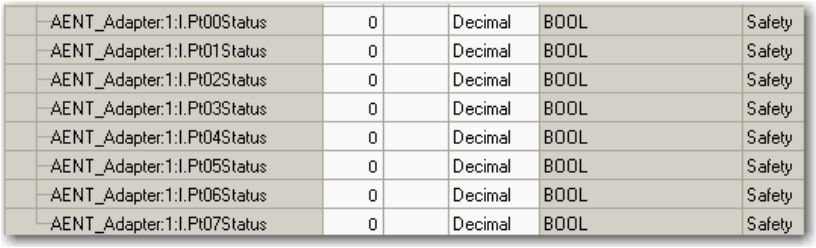


AENT_Adapter:1:O	{...}	{...}		AB:1734_IB8S:O:0	Safety
AENT_Adapter:1:O.Test00Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:O.Test01Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:O.Test02Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:O.Test03Data	0		Decimal	BOOL	Safety

a. Damit diese Option im Pulldown-Menü zur Verfügung steht, müssen Sie im Pulldown-Menü „Configured By“ (Konfiguriert von) die Option „This Controller“ (Diese Steuerung) auswählen.

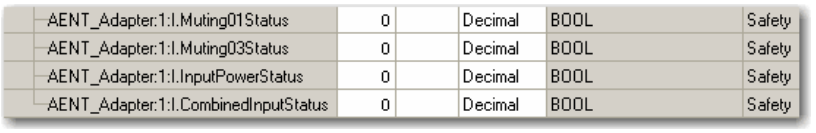
14. Wählen Sie im Pulldown-Menü „Input Status“ (Eingangsstatus) die gewünschte Methode für das Eingangsmodul aus:

Auswahl	Beschreibung
None (Keine)	Es gibt keine Status-Tags, nur Daten für die Eingänge.
Pt. Status (Punktstatus)	Es gibt ein Status-Tag für jeden Eingangspunkt.



AENT_Adapter:1:I.Pt00Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt01Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt02Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt03Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt04Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt05Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt06Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt07Status	0		Decimal	BOOL	Safety

Combined Status – Muting (Kombinierter Status – Muting)	• Ein einzelnes BOOLESCHES Tag stellt ein UND des Status-Bits für alle Eingangspunkte dar. Wenn beispielsweise ein Fehler an einem Eingangskanal vorliegt, wechselt das Bit nach LO.[a] • Ein einzelnes BOOLESCHES Tag stellt den Status der Eingangsleistung (Fehler-Bit) der Eingangsbaugruppe dar. • Ein Muting-Status-Tag für Testausgang T1 und T3.



AENT_Adapter:1:I.Muting01Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Muting03Status	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.InputPowerStatus	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.CombinedInputStatus	0		Decimal	BOOL	Safety

Auswahl	Beschreibung
Pt. Status – Muting (Punktstatus – Muting)	Es gibt ein Muting-Status-Tag für Testausgang T1 und T3 mit einem Punktstatus für jeden Eingangspunkt.

Adapter:1:I.Pt00Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt01Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt02Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt03Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt04Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt05Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt06Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt07Status	0		Decimal	BOOL	Safety
Adapter:1:I.Muting01Status	0		Decimal	BOOL	Safety
Adapter:1:I.Muting03Status	0		Decimal	BOOL	Safety
Adapter:1:I.InputPowerStatus	0		Decimal	BOOL	Safety

Pt. Status – Muting-Test Output (Punktstatus – Muting-Test-Ausgang)	• Status-Tags für alle Eingangspunkte. • Muting-Status-Tag für Testausgang T1 und T3. • Status-Tags für alle Testausgänge.

Adapter:1:I.Pt00Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt01Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt02Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt03Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt04Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt05Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt06Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt07Status	0		Decimal	BOOL	Safety
Adapter:1:I.Pt00TestOutputStatus	0		Decimal	BOOL	Safety
Adapter:1:I.Pt01TestOutputStatus	0		Decimal	BOOL	Safety
Adapter:1:I.Pt02TestOutputStatus	0		Decimal	BOOL	Safety
Adapter:1:I.Pt03TestOutputStatus	0		Decimal	BOOL	Safety
Adapter:1:I.Muting01Status	0		Decimal	BOOL	Safety
Adapter:1:I.Muting03Status	0		Decimal	BOOL	Safety
Adapter:1:I.InputPowerStatus	0		Decimal	BOOL	Safety

a. Bei Verwendung des kombinierten Status verwenden Sie die explizite Nachrichtenübertragung zum Lesen des Status der einzelnen Punkte zu Diagnosezwecken.

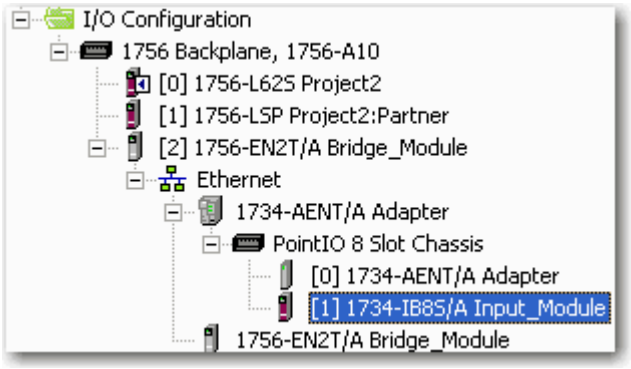
15. Wählen Sie im Pulldown-Menü „Data Format“ (Datenformat) den Standardwert „Integer“ (Ganzzahl) aus.

16. Klicken Sie auf OK.

Sie kehren in das Dialogfeld „Module Properties“ (Moduleigenschaften) zurück.

17. Klicken Sie auf OK, um Ihre Änderungen anzuwenden.

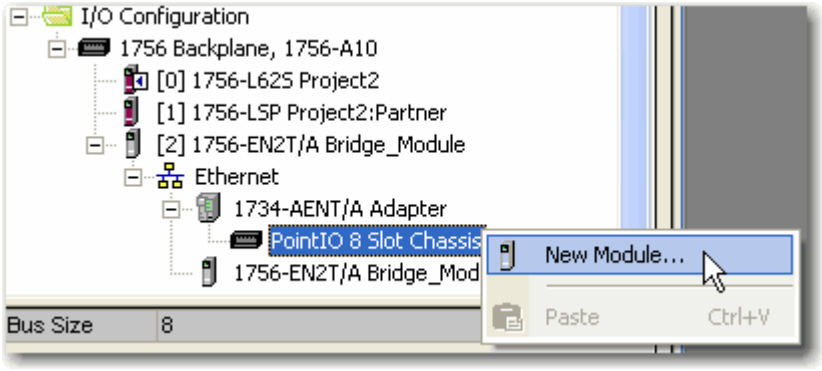
Im E/A-Konfigurationsbaum wird das 1734-IB8S-Modul angezeigt.



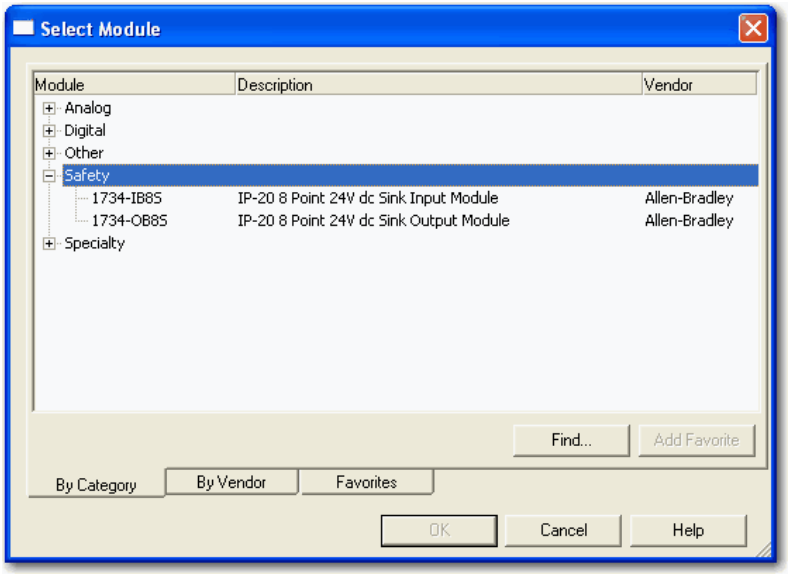
Hinzufügen und Konfigurieren von Sicherheitsausgangsmodulen

Gehen Sie wie folgt vor, um POINT Guard I/O-Sicherheitsmodule hinzuzufügen und zu konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf das POINT I/O-Chassis, und wählen Sie „New Module“ (Neues Modul) aus.

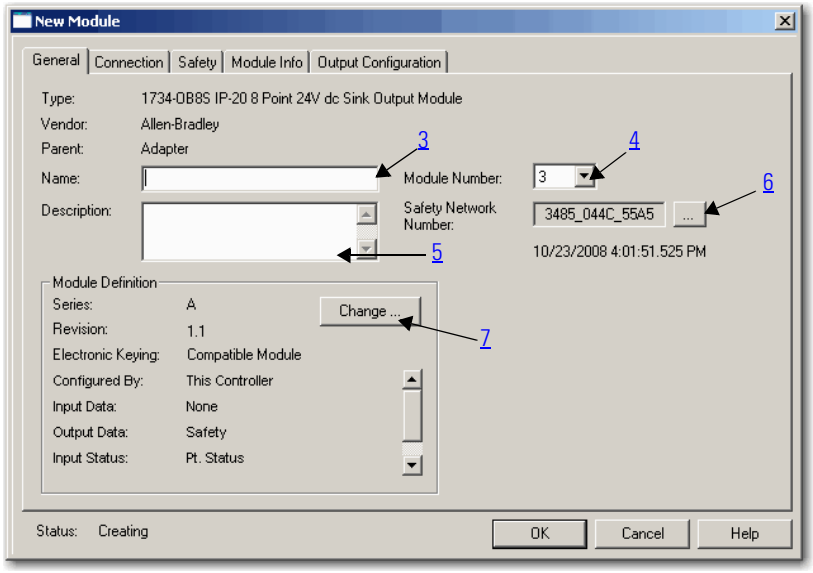


Das Dialogfeld „Select Module“ (Modul auswählen) wird mit einer Liste angezeigt, die u. a. den Punkt „Safety“ (Sicherheit) enthält.



2. Wählen Sie das gewünschte Ausgangsmodul aus, z. B. 1734-OB8S, und klicken Sie auf OK.

Das Dialogfeld „New Module“ (Neues Modul) wird angezeigt.



3. Geben Sie in das Feld „Name“ einen eindeutigen Namen für das Ausgangsmodul ein.

4. Geben Sie in das Feld „Module Number“ (Modulnummer) eine eindeutige Modulnummer für das Ausgangsmodul ein.

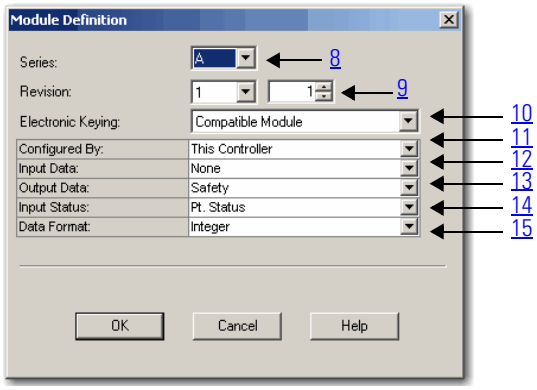
5. Geben Sie in das Feld „Description“ (Beschreibung) eine Beschreibung des Ausgangsmoduls ein, wenn Sie dies wünschen.

6. Verwenden Sie im Feld „Safety Network Number“ (Sicherheitsnetzwerknummer) die Standardeinstellung.

   Eine ausführliche Erläuterung der Sicherheitsnetzwerknummer (SNN) finden Sie in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch. In den meisten Fällen verwenden Sie die von der Software RSLogix 5000 vorgeschlagene Standardeinstellung.

7. Klicken Sie auf „Change“ (Ändern), um die Moduldefinition zu bearbeiten.

   Das Dialogfeld „Module Definition“ (Moduldefinition) wird angezeigt.



8. Geben Sie in das Feld „Series“ (Serie) den Serienbuchstaben des Ausgangsmoduls ein.

9. Geben Sie in die Felder „Revision“ (Version) die Versionsnummern des Ausgangsmoduls ein.

10. Wählen Sie im Pulldown-Menü „Electronic Keying“ (Elektronische Codierung) die gewünschte Codierungsmethode für das Ausgangsmodul aus folgenden Optionen aus:

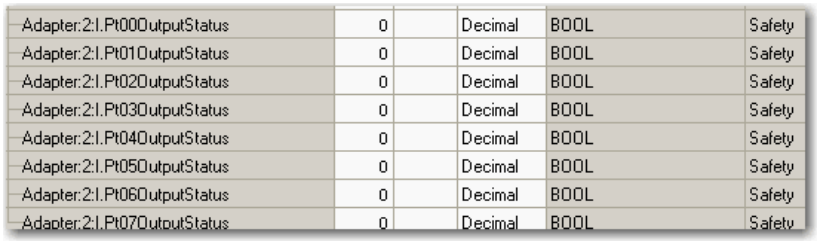
Auswahl	Beschreibung
Exact Match (Exakte Übereinstimmung)	Alle Parameter müssen übereinstimmen, da anderenfalls das eingesetzte Modul eine Verbindung zur Steuerung zurückweist.
Compatible Module (Kompatibles Modul)	Mit dieser Option kann ein E/A-Modul feststellen, ob es das Modul, das in der von der Steuerung gesendeten Konfiguration definiert ist, emulieren kann.

11. Wählen Sie im Pulldown-Menü „Configured By“ (Konfiguriert von) die gewünschte Konfigurationsmethode für dieses Modul aus folgenden Optionen aus.

Auswahl	Beschreibung
This Controller (Diese Steuerung)	Mit dieser Auswahl wird die Steuerung angewiesen, die Sicherheitsausgänge zu konfigurieren und zu steuern. Die Auswahl „Output Data“ (Ausgangsdaten) wird auf „Safety“ (Sicherheit) gesetzt.
External Means (Externe Mittel)	Mit dieser Auswahl wird die Steuerung angewiesen, ausschließlich eine Sicherheitseingangsverbindung herzustellen. Die Steuerung konfiguriert das Modul nicht und kann auch die Sicherheitsausgänge nicht steuern. Die Auswahl „Output Data“ (Ausgangsdaten) wird auf „None“ (Keine) gesetzt.

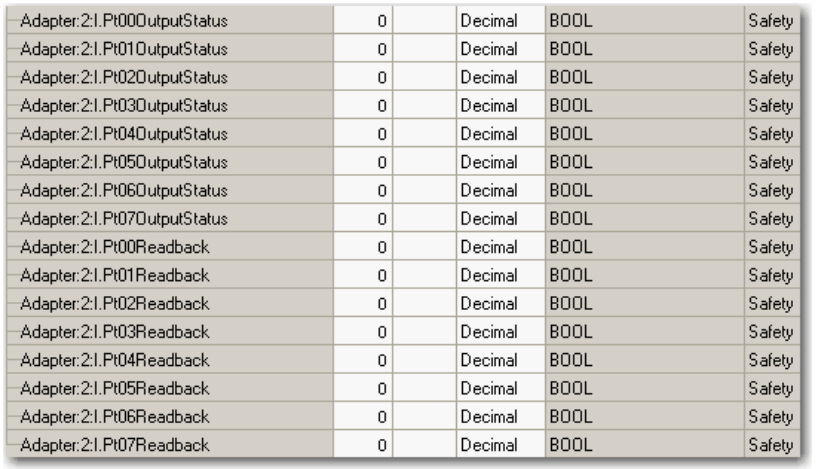
12. Wählen Sie im Pulldown-Menü „Input Status“ (Eingangsstatus) die gewünschte Methode für das Ausgangsmodul aus:

Auswahl	Beschreibung
Pt. Status (Punktstatus)	Es gibt ein Status-Tag für jeden Eingangs- und Ausgangspunkt.



Adapter:2:I.Pt00OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt01OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt02OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt03OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt04OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt05OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt06OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt07OutputStatus	0		Decimal	BOOL	Safety

Point Status – Readback (Punktstatus – Rücklesung)	Diese Option steht nur für Sicherheitsmodule zur Verfügung, die ausschließlich über Ausgänge verfügen. Durch Auswahl von „Point Status – Readback“ (Punktstatus – Rücklesung) werden Ausgangsstatus- und Rücklese-Tags erstellt, wobei Rücklese-Tags auf das Vorhandensein einer Spannung von 24 V an der Ausgangsklemme hinweisen.



Adapter:2:I.Pt00OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt01OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt02OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt03OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt04OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt05OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt06OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt07OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt00Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt01Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt02Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt03Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt04Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt05Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt06Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt07Readback	0		Decimal	BOOL	Safety

Auswahl	Beschreibung
Combined Status – Readback – Power (Kombinierter Status – Rücklesung – Spannung)	• Ein einzelnes BOOLESCHES Tag stellt ein UND des Status-Bits für alle Ausgangspunkte dar. Wenn beispielsweise ein Fehler an einem Ausgangskanal vorliegt, wechselt das Bit nach LO.[a] • Durch Auswahl von „Readback" (Rücklesung) werden Ausgangsstatus- und Rücklese-Tags erstellt, wobei Rücklese-Tags auf das Vorhandensein einer Spannung von 24 V an der Ausgangsklemme hinweisen. • Ein einzelnes BOOLESCHES Tag stellt den Status der Ausgangsleistung (Fehler-Bit) der Ausgangsbaugruppe dar.

Adapter:2:I.Pt00Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt01Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt02Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt03Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt04Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt05Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt06Readback	0		Decimal	BOOL	Safety
Adapter:2:I.Pt07Readback	0		Decimal	BOOL	Safety
Adapter:2:I.OutputPowerStatus	0		Decimal	BOOL	Safety
Adapter:2:I.CombinedOutputStatus	0		Decimal	BOOL	Safety

a. Bei Verwendung des kombinierten Status verwenden Sie die explizite Nachrichtenübertragung zum Lesen des Status der einzelnen Punkte zu Diagnosezwecken.

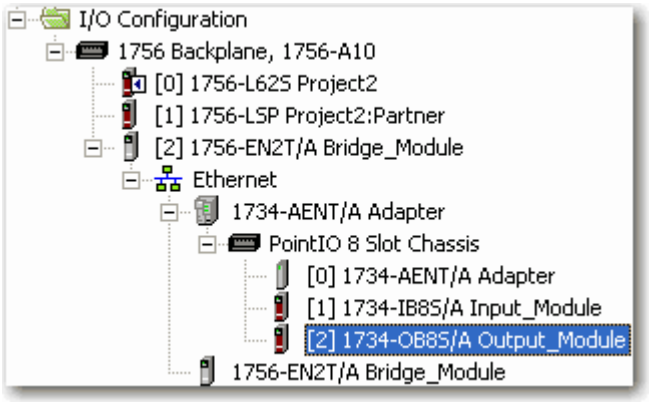
13. Wählen Sie im Pulldown-Menü „Data Format" (Datenformat) den Standardwert „Integer" (Ganzzahl) aus.

14. Klicken Sie auf OK.

Sie kehren in das Dialogfeld „Module Properties" (Moduleigenschaften) zurück.

15. Klicken Sie auf OK, um Ihre Änderungen anzuwenden.

Im E/A-Konfigurationsbaum wird das 1734-OB8S-Modul angezeigt.



Werte und Zustände von Tags

In dieser Tabelle sind die Werte und Zustände der Tags aufgelistet.

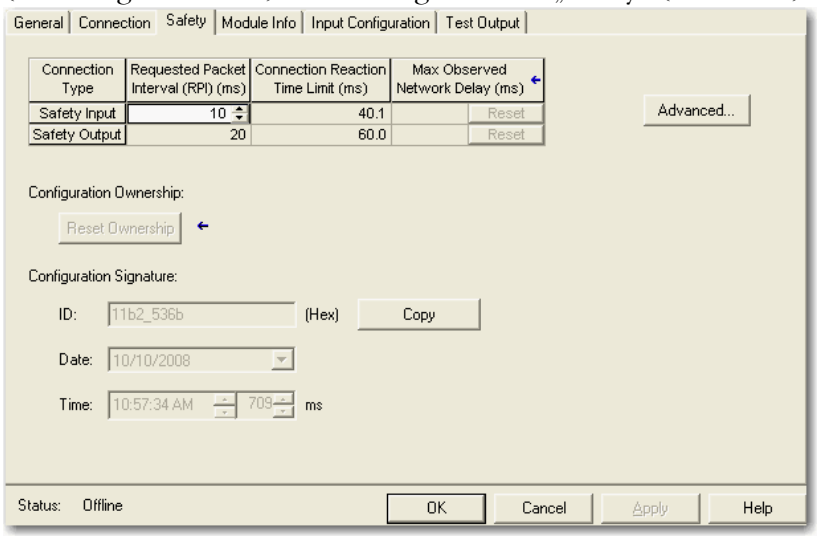
Daten		Beschreibung
Eingangs-daten	Sicherheitseingangsdaten SICHERHEIT	Gibt den EIN/AUS-Zustand der einzelnen Eingangsschaltungen an. • EIN: 1 AUS: 0
	Kombinierter Sicherheitseingangsstatus – SICHERHEIT	Ein UND des Status aller Eingangsschaltungen. • Alle Schaltkreise weisen den Normalzustand auf: 1 • In mindestens einer Eingangsschaltung wurde ein Fehler erkannt: 0
	Individueller Sicherheitseingangsstatus – SICHERHEIT	Gibt den Status der einzelnen Eingangsschaltungen an. • Normal: 1 Fehler (Alarm): 0
	Kombinierter Sicherheitsausgangsstatus – SICHERHEIT	Ein UND des Status aller Sicherheitsausgangsschaltungen. • Alle Schaltkreise weisen den Normalzustand auf: 1 • In mindestens einer Ausgangsschaltung wurde ein Fehler erkannt: 0
	Individueller Sicherheitsausgangsstatus – SICHERHEIT)	Gibt den Status der einzelnen Sicherheitsausgangsschaltungen an. • Normal: 1 Fehler (Alarm): 0
	Muting-Leuchten-Status – SICHERHEIT	Gibt den Status an, wenn die Schaltkreise T1 und T3 als Muting-Leuchten-Ausgänge konfiguriert sind. • Normal: 1 Fehler (Alarm): 0
	Rücklesung des Ausgangs – STANDARD	Überwacht das Vorhandensein von 24 V an der Ausgangsschaltung. Das Rücklesen ist aktiviert (1), wenn an der Ausgangsklemme 24 V anliegen. • EIN: 1 AUS: 0
	Individueller Testausgangsstatus – STANDARD	Gibt den Status der einzelnen Testausgangsschaltungen an. • Normal: 1 Fehler (Alarm): 0
	Fehler-Bit Eingangsleistung	Gibt an, dass der bereitgestellte Feldstrom innerhalb der Spezifikationen liegt. • Stromfehler: 1 Strom OK: 0
	Fehler-Bit Ausgangsleistung	Gibt an, dass der bereitgestellte Feldstrom innerhalb der Spezifikationen liegt. • Stromfehler: 1 Strom OK: 0
Ausgangs-daten	Sicherheitsausgangsdaten – SICHERHEIT	Steuert den Sicherheitsausgang. • EIN: 1 AUS: 0
	Standardausgangsdaten – STANDARD	Steuert den Testausgang, wenn der Testausgangsmodus auf einen Standardausgang gesetzt ist. • EIN: 1 AUS: 0

WICHTIG „Sicherheit“ weist auf Informationen hin, die die Steuerung in sicherheitsrelevanten Funktionen verwenden kann. „Standard“ weist auf zusätzliche Informationen hin, auf die Sie sich für Sicherheitsfunktionen nicht verlassen dürfen.

Konfigurieren der Registerkarte „Safety“ (Sicherheit)

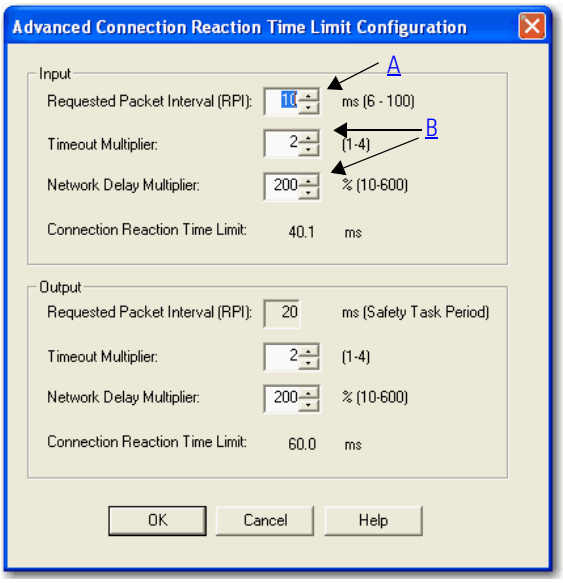
Dieser Abschnitt enthält Informationen zum Ausfüllen der Felder auf der Registerkarte „Safety“ (Sicherheit).

1. Klicken Sie im Dialogfeld „Module Properties“ (Moduleigenschaften) auf die Registerkarte „Safety“ (Sicherheit).



2. Klicken Sie auf „Advanced“ (Erweitert).

Das Dialogfeld „Advanced Connection Reaction Time Limit Configuration“ (Erweiterte Konfiguration des Grenzwerts für die Verbindungsreaktionszeit) wird angezeigt.



Weitere Informationen zum Dialogfeld „Advanced Connection Reaction Time Limit Configuration“ finden Sie in der Publikation 1756-UM020, GuardLogix-Steuerungen – Benutzerhandbuch.

A. Geben Sie in das Feld „Requested Packet Interval (RPI)“ (Angefordertes Paketintervall (RPI)) das RPI für die Eingangsverbindung Ihrer Anwendung ein (der Wert muss zwischen 6 und 500 ms liegen).

Das kleinste zulässige Eingangs-RPI ist 6 ms. Die Auswahl kleiner RPIs beansprucht die Netzwerkbandbreite mehr und kann zu Fehlerauslösungen führen, da andere Geräte keinen Zugriff auf das Netzwerk erhalten.

Beispielsweise funktioniert ein Sicherheitseingangsmodul, an dem ausschließlich Not-Halt-Schalter angeschlossen sind, im Allgemeinen problemlos mit einer Einstellung zwischen 50 und 100 ms. Ein Eingangsmodul mit einem Lichtgitter, das vor Gefahren schützt, erfordert eventuell die schnellstmögliche Reaktionszeit.

Die Auswahl der richtigen RPIs führt zu einem System mit maximaler (bester) Leistung.

B. Verwenden Sie die Standardwerte für „Timeout Multiplier“ (Timeout-Multiplikator) (2) und „Network Delay Multiplier“ (Netzwerkverzögerungs-Multiplikator) (200).

WICHTIG

Analysieren Sie alle Sicherheitskanäle, um die erforderlichen Einstellungen zu bestimmen. Die Standardwerte für den Timeout-Multiplikator (2) und den Netzwerkverzögerungs-Multiplikator (200) sorgen für ein Reaktionszeitlimit der Eingangsverbindung, das das Vierfache des RPI beträgt, und für ein Reaktionszeitlimit der Ausgangsverbindung, das das Dreifache des RPI beträgt. Änderungen an diesen Parametern müssen von einem Sicherheitsadministrator genehmigt werden.

Es liegt ein Verbindungsstatus-Tag für jede Verbindung vor.

AENT_Adapter:1:I	{...}	{...}		AB:1734_IB8S_Safety5:I:0	Safety
AENT_Adapter:1:I.RunMode	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.ConnectionFaulted	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt00Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt01Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt02Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt03Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt04Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt05Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt06Data	0		Decimal	BOOL	Safety
AENT_Adapter:1:I.Pt07Data	0		Decimal	BOOL	Safety

Falls das RPI und das Zeitlimit für die Verbindungsreaktionszeit des Netzwerks entsprechend festgelegt wurden, muss dieses Status-Tag stets auf HI gesetzt bleiben. Überwachen Sie alle Verbindungsstatus-Bits, um sicherzustellen, dass sie aufgrund von Timeouts nicht vorübergehend nach LO wechseln.

Verwaltungsrechte für die Konfiguration

Die Verbindung zwischen der verwaltenden Steuerung und dem POINT Guard I/O-Modul basiert auf Folgendem:

- POINT Guard I/O-Modulnummer
- POINT Guard I/O-Sicherheitsnetzwerknummer
- GuardLogix-Steckplatznummer
- GuardLogix-Sicherheitsnetzwerknummer
- Pfad von der GuardLogix-Steuerung zum POINT Guard I/O-Modul
- Konfigurationssignatur

Ändert sich einer dieser Werte, wird die Verbindung zwischen der GuardLogix-Steuerung und dem POINT Guard I/O-Modul unterbrochen, und in der RSLogix 5000-Verzeichnisstruktur wird das gelbe Symbol angezeigt. Weitere Informationen finden Sie in Kapitel 8.

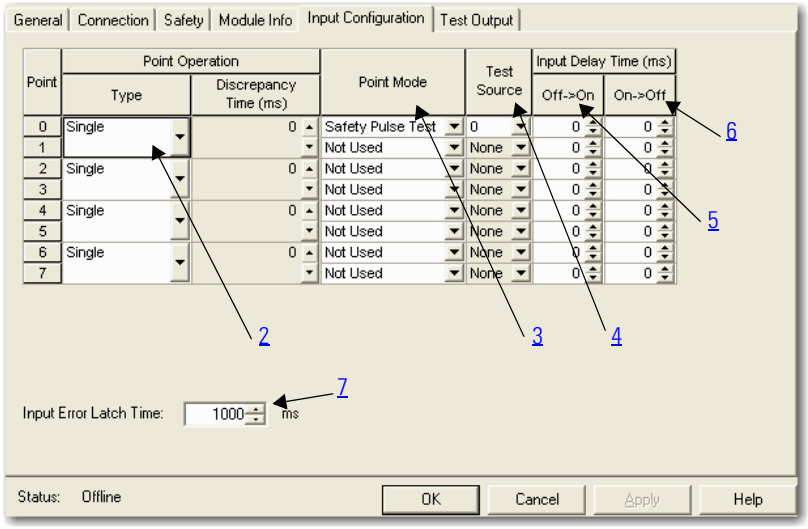
Konfigurationssignatur

Die Konfigurationssignatur wird von der Software RSLogix 5000 erstellt und vom POINT Guard I/O Module verifiziert. Die Konfigurationssignatur stellt die SIL3-Integrität der Konfiguration eines POINT Guard I/O-Moduls zur Verfügung. Ausführliche Informationen zur Konfigurationssignatur finden Sie in der Publikation 1756-UM020, GuardLogix-Steuerungen – Benutzerhandbuch.

Konfigurieren der Registerkarte „Input Configuration“ (Eingangskonfiguration)

Gehen Sie wie folgt vor, um die Eingangskonfiguration abzuschließen. Weitere Informationen hierzu finden Sie in Kapitel 2.

1. Klicken Sie im Dialogfeld „Module Properties“ (Moduleigenschaften) auf die Registerkarte „Input Configuration“ (Eingangskonfiguration).



2. Ordnen Sie die Art des Punktbetriebs zu.

   Wenn Sie „Equivalent“ (Gleichwertig) oder „Complementary“ (Komplementär) auswählen, müssen Sie darüber hinaus eine entsprechende Diskrepanzzeit zuordnen.

Auswahl	Beschreibung
Single (Einzeln)	Eingänge werden als Einzelkanäle behandelt. Beachten Sie, dass in vielen Fällen zweikanalige Sicherheitseingänge als zwei individuelle Einzelkanäle konfiguriert sind. Dies hat keinerlei Auswirkungen auf Impulstests, da diese für einzelne Kanäle ausgeführt werden.
Equivalent (Gleichwertig)[a]	Eingänge werden als zweikanaliges Paar behandelt. Die Kanäle müssen innerhalb der Diskrepanzzeit übereinstimmen, da anderenfalls ein Fehler generiert wird.
Complementary (Komplementär)[(a)]	Eingänge werden als zweikanaliges Paar behandelt. Sie müssen innerhalb der Diskrepanzzeit gegensätzliche Zustände aufweisen, da anderenfalls ein Fehler generiert wird.

a. Beachten Sie, dass durch die Konfiguration einer Diskrepanzzeit für Sicherheits-E/A-Module Eingangsdiskrepanzen maskiert und von den Sicherheitsbefehlen der Steuerung erkannt werden. Der Status kann von der Steuerung gelesen werden, um diese Fehlerinformationen abzurufen.

Eine Diskrepanzzeiteinstellung von 0 ms bedeutet, dass die Kanäle in einer zweikanaligen Konfiguration für unbestimmte Zeit abweichen können, ohne dass ein Fehler angezeigt wird.

Bei einer Diskrepanzzeit von 0 ms wechselt der evaluierte Status der Eingänge aufgrund einer erforderlichen Bedingung „Cycle Inputs“ (Eingänge aus- und wieder einschalten) ebenfalls in den Sicherheitszustand, doch da die Diskrepanzzeit auf 0 ms eingestellt ist, wird kein Fehler angezeigt.

Die erforderliche Bedingung „Cycle Inputs“ (Eingänge aus- und wieder einschalten) liegt vor, wenn eine Eingangsklemme von ihrem normalen aktiven Zustand in den inaktiven und dann wieder in den aktiven Zustand wechselt, während die andere Eingangsklemme ihren normalen aktiven Zustand beibehält. Auch wenn kein Fehler angezeigt wird, müssen die Eingänge dennoch aus- und wieder eingeschaltet werden, bevor sie wieder in den aktiven Zustand zurückkehren können.

Doch wenn sich die Kanäle vor der Diskrepanz im aktiven Zustand befunden haben und am Ende wieder in den aktiven Zustand wechseln, liegt eine erforderliche Bedingung „Cycle Input“ vor, die **nicht** deklariert wird. Der logische Zustand stimmt **nicht** mit der Spannung an den Klemmen überein. Die Kanäle müssen über den Sicherheitszustand aus- und wieder eingeschaltet werden, bevor sie wieder in den aktiven Zustand zurückkehren.

3. Ordnen Sie den Punktmodus zu.

Auswahl	Beschreibung
Not Used (Nicht verwendet)	Der Eingang ist deaktiviert. Er verbleibt logisch 0, wenn an der Eingangsklemme 24 V angelegt werden.
Safety Pulse Test (Sicherheitsimpulstest)	An dieser Eingangsschaltung werden Impulstests durchgeführt. Eine Testquelle am POINT Guard I/O-Modul **muss** als 24-V-Quelle für diesen Schaltkreis verwendet werden. Die Testquelle wird mithilfe des Pulldown-Menüs „Test Source“ (Testquelle) konfiguriert. Der Impulstest erkennt Kurzschlüsse an 24 V und Kurzschlüsse zwischen Kanälen an anderen Eingängen.
Sicherheit	Ein Sicherheitseingang ist angeschlossen, doch das POINT Guard I/O-Modul muss für diesen Schaltkreis keinen Impulstest ausführen. Ein Beispiel hierfür ist ein Sicherheitsgerät, das seine eigenen Impulstests an den Eingangsdrähten ausführt, wie z. B. ein Lichtgitter.
Standard	Es ist ein Standardgerät, wie z. B. ein Reset-Schalter, angeschlossen. Dieser Punkt kann nicht im zweikanaligen Betrieb verwendet werden.

4. Ordnen Sie die Testquelle jedem Sicherheitseingang am Modul zu, für den Sie Impulstests ausführen möchten.

Auswahl	Beschreibung
None (Keine)	Falls an einem Eingangspunkt Impulstests ausgeführt werden, muss die Testquelle, welche die 24 V für die Eingangsschaltung liefert, ausgewählt werden. Wird die falsche Testquelle eingegeben, kommt es an dieser Eingangsschaltung zu Impulstestfehlern.
Test Output 0 (Testausgang 0)	
Test Output 1 (Testausgang 1)[a]	
Test Output 2 (Testausgang 2)	
Test Output 3 (Testausgang 3)[(a)]	

a. Die Testausgänge 1 und 3 sind mit einer optionale Muting-Funktionalität ausgestattet.

5. Ordnen Sie die Eingangsverzögerungszeit zu, Aus -> Ein (0–126 ms, in Inkrementen von 6 ms).

   Filterzeit für die Transition von AUS nach EIN. Der Eingang muss nach Ablauf der Eingangsverzögerung den Zustand HI aufweisen, bevor er auf den Wert einer logischen 1 gesetzt wird. Diese Verzögerungszeit wird pro Kanal konfiguriert, wobei jeder Kanal speziell an die Leistungsmerkmale des Feldgeräts angepasst wird, um die Leistung zu maximieren.

6. Ordnen Sie die Eingangsverzögerungszeit zu, Aus -> Ein (0–126 ms, in Inkrementen von 6 ms).

   Filterzeit für die Transition von EIN nach AUS. Der Eingang muss nach Ablauf der Eingangsverzögerung den Zustand LO aufweisen, bevor er auf den Wert einer logischen 0 gesetzt wird. Diese Verzögerungszeit wird pro Kanal konfiguriert, wobei jeder Kanal speziell an die Leistungsmerkmale des Feldgeräts angepasst wird, um die Leistung zu maximieren.

7. Geben Sie in das Feld „Input Error Latch Time“ (Selbsthaltezeit für Eingangsfehler) ein, wie lange das Modul einen Fehler hält, um sicherzustellen, dass die Steuerung diesen erkennen kann (0–65 530 ms, in Inkrementen von 10 ms – Standardwert 1000 ms).

Auf diese Weise erhalten Sie zuverlässigere Diagnosen, und Fehlerauslösungen werden eher erkannt. Die Selbsthaltung von Eingangsfehlern soll sicherstellen, dass unstetige Fehler, die lediglich einige Millisekunden lang vorliegen, lange genug gehalten werden, damit sie die Steuerung lesen kann. Wie lange die Fehler gehalten werden, hängt vom RPI, dem Überwachungszeitraum der Sicherheits-Task und anderen anwendungsspezifischen Variablen ab.

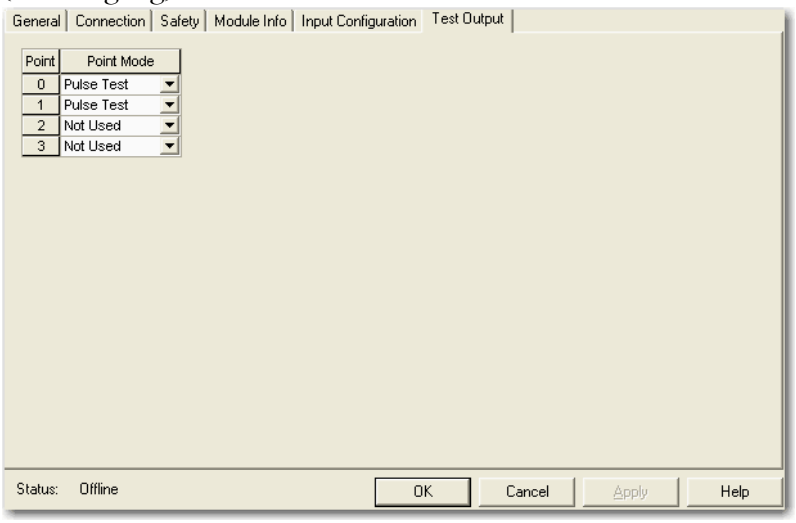
8. Klicken Sie auf „Apply“ (Übernehmen).

Konfigurieren der Registerkarte „Test Output“ (Testausgang)

In diesem Abschnitt sind die Funktionen des Dialogfelds „Test Output Configuration“ (Konfiguration des Testausgangs) beschrieben. Informationen zum Konfigurieren der Testausgänge finden Sie in dieser Tabelle.

Gehen Sie wie folgt vor, um die Testausgangskonfiguration abzuschließen.

1. Klicken Sie im Dialogfeld „Module Properties“ (Moduleigenschaften) auf die Registerkarte „Test Output“ (Testausgang).



2. Ordnen Sie den Punktmodus zu.

Auswahl	Beschreibung
Not Used (Nicht verwendet) (Standardwert)	Der Testausgang ist deaktiviert.
Standard	Der Testausgangspunkt kann von der GuardLogix-Steuerung programmatisch gesteuert werden.
Pulse Test (Impulstest)	Der Testausgang wird als Impulstestquelle verwendet.
Power Supply (Netzteil)	Eine konstante 24-V-Spannung liegt an der Ausgangsklemme an. Sie kann verwendet werden, um ein Feldgerät mit Spannung zu versorgen.
Muting Lamp Output (Ausgang Muting-Leuchte) (nur Klemme T1 und T3)	Am Ausgang ist eine Anzeigeleuchte angeschlossen. Wenn diese Leuchte eingeschaltet ist, kann eine durchgebrannte Glühlampe, ein Drahtbruch oder ein Erdschluss erkannt werden. In der Regel wird die Leuchte als Anzeige in Lichtgitteranwendungen verwendet.

Außerdem steht der Parameter „Test Output Fault Action“ (Aktion bei Testausgangsfehler) zur Verfügung, der nur über die explizite Nachrichtenübertragung gelesen oder geschrieben werden kann. Wenn ein Zeitfehler der Kommunikation auftritt, können Sie die

Testausgänge auf „Clear OFF“ (AUS löschen) (Standardwert) oder „Hold Last State“ (Letzten Zustand halten) setzen. Weitere Informationen finden Sie auf Anhang A.

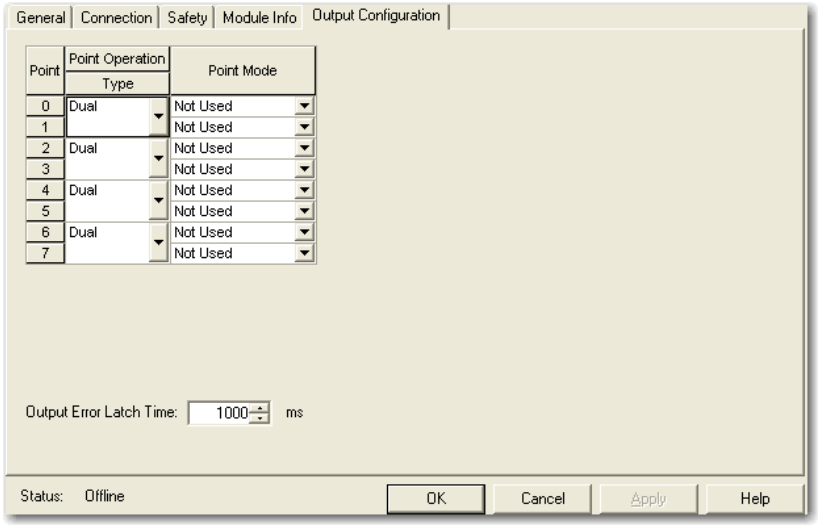
3. Klicken Sie auf „Apply“ (Übernehmen).

Konfigurieren der Registerkarte „Output Configuration“ (Ausgangskonfiguration)

Dieser Abschnitt enthält Anweisungen zum Konfigurieren der Sicherheitsausgänge. Füllen Sie die Felder mithilfe der Informationen in dieser Tabelle aus, und orientieren Sie sich dabei an der Abbildung.

Gehen Sie wie folgt vor, um die Sicherheitsausgangskonfiguration abzuschließen.

1. Klicken Sie im Dialogfeld „Module Properties“ (Moduleigenschaften) auf die Registerkarte „Output Configuration“ (Ausgangskonfiguration).



2. Ordnen Sie die Art des Punktbetriebs zu.

Auswahl	Beschreibung
Single (Einzeln)[a]	Der Ausgang wird wie ein einzelner Kanal behandelt.
Dual (Standard)	Das POINT Guard I/O-Modul behandelt die Ausgänge als Paar. Es setzt sie stets als übereinstimmendes Paar auf HI oder LO. Die Sicherheitslogik muss diese beiden Ausgänge gleichzeitig auf EIN oder AUS setzen, da ansonsten das Modul einen Kanalfehler ausgibt.

a. Dies gilt nicht für bipolare Ausgänge.

3. Ordnen Sie den Punktmodus zu.

Auswahl	Beschreibung
Not Used (Nicht verwendet)	Der Ausgang ist deaktiviert.
Sicherheit	Der Ausgangspunkt ist aktiviert und führt am Ausgang keinen Impulstest aus.
Safety Pulse Test (Sicherheitsimpulstest)	Der Ausgangspunkt ist aktiviert und führt einen Impulstest am Ausgang aus. Wenn der Ausgang eingeschaltet ist, gibt der Ausgang einen kurzen LO-Impuls aus. Der Impulstest erkennt, wenn an der Ausgangsklemme während dieses LO-Impulses weiterhin eine Spannung von 24 V anliegt. Der Grund hierfür kann ein Kurzschluss an 24 V oder ein Kurzschluss des Ausgangs an einer anderen Ausgangsklemme sein.

4. Geben Sie in das Feld „Output Error Latch Time“ (Selbsthaltezeit für Ausgangsfehler) ein, wie lange das Modul einen Fehler hält, um sicherzustellen, dass die Steuerung diesen erkennen kann (0–65 530 ms, in Inkrementen von 10 ms – Standardwert 1000 ms).

Auf diese Weise erhalten Sie zuverlässigere Diagnosen, und Fehlerauslösungen werden eher erkannt.

Die Selbsthaltung von Ausgangsfehlern soll sicherstellen, dass unstetige Fehler, die lediglich einige Millisekunden lang vorliegen, lange genug gehalten werden, damit sie die Steuerung lesen kann. Wie lange die Fehler gehalten werden, hängt vom RPI, dem Überwachungszeitraum der Sicherheits-Task und anderen anwendungsspezifischen Variablen ab.

5. Klicken Sie auf „Apply“ (Übernehmen).

Speichern und Herunterladen der Modulkonfiguration

Es wird empfohlen, Ihre Arbeit nach der Konfiguration eines Moduls zu speichern.

Wenn nach dem Herunterladen des Programms die Statusanzeigen MS und NS am POINT Guard I/O-Modul nicht beide konstant grün leuchten, sind eventuell die Verwaltungsrechte verloren gegangen. Die Verwaltungsrechte basieren auf Folgendem:

- POINT Guard I/O-Modulnummer
- POINT Guard I/O-Sicherheitsnetzwerknummer
- GuardLogix-Steckplatznummer
- GuardLogix-Sicherheitsnetzwerknummer
- Pfad von der GuardLogix-Steuerung zum POINT Guard I/O-Modul
- Konfigurationssignatur

Ändert sich einer dieser Werte, wird die Verbindung zwischen der GuardLogix-Steuerung und dem POINT Guard I/O-Modul unterbrochen, und in der RSLogix 5000-Verzeichnisstruktur wird ein gelbes Symbol angezeigt. Weitere Informationen finden Sie in Kapitel 8.

Konfiguration des Moduls für eine SmartGuard-Steuerung

Thema	Seite
Einleitung	107
Vorbereitungen	107
Verwenden der Hilfe	108
Arbeiten mit der Software RSNetWorx for DeviceNet	108
Einrichten der Sicherheitskonfiguration	110
Konfigurieren Sie die Eingangs- und Ausgangsverbindungen der SmartGuard-Steuerung	116
Speichern und Herunterladen der Modulkonfiguration	121

Einleitung

Dieses Kapitel enthält Informationen zum Konfigurieren einer SmartGuard-Steuerung und von POINT Guard I/O-Modulen über die USB-Anschlüsse (Universal Serial Bus). Informationen zur Bedienung des Netzwerkkonfigurators finden Sie in den Hilfedateien der Software RSNetWorx for DeviceNet.

Vorbereitungen

Vergewissern Sie sich, dass die folgenden Komponenten vorhanden sind:

- Software RSNetWorx for DeviceNet, Version 9.0 oder höher
- RSLinx-Software, Version 2.51 oder höher
- SmartGuard USB-Treiber

  Der SmartGuard USB-Treiber muss bereits in Ihrer RSLinx-Software vorhanden sein. Ist dies nicht der Fall, laden Sie den Treiber auf Ihren Computer, und notieren Sie sich den Ordner, da Sie später auf diesen Ordner zurückgreifen müssen.

- PC mit dem Betriebssystem Microsoft Windows 2000, Microsoft Windows 2000 Terminal Server oder Microsoft Windows XP
- 1734-PDN-Adapter

- 1734-IB8S- und/oder 1734-OB8S-EDS-Files

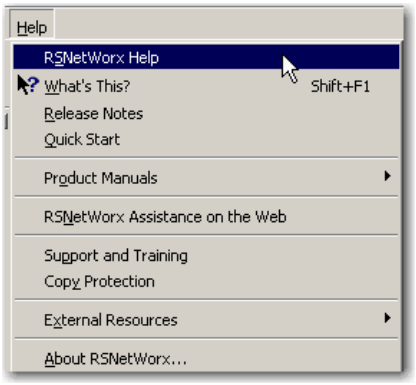
TIPP

Die entsprechenden EDS-Files können Sie auf der EDS-Hardware- und Installations-Website unter http://www.rockwellautomation.com/resources/eds/ herunterladen.

Das EDS-File für das Modul 1734-IB8S ist 0010023000F0100. Das EDS-File für das Modul 1734-OB8S ist 001002300100100F0100.

Verwenden der Hilfe

Informationen zur RSNetWorx for DeviceNet-Software erhalten Sie im Hilfemenü über die Option „RSNetWorx Help“ (Hilfe zu RSNetWorx).



Arbeiten mit der Software RSNetWorx for DeviceNet

Gehen Sie wie folgt vor, bevor Sie ein Projekt mit der Software RSNetWorx for DeviceNet entwickeln:

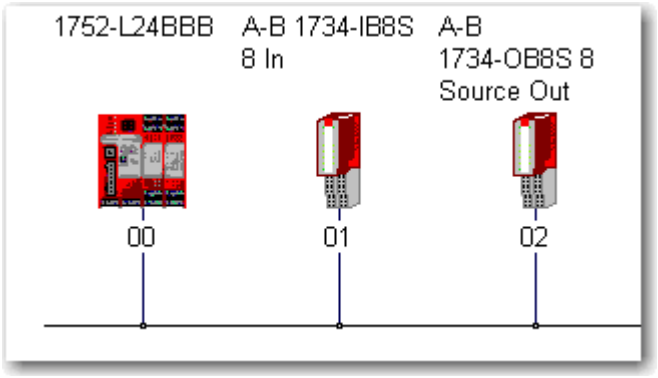
1. Laden Sie die richtigen EDS-Files (Electronic Data Sheet) mithilfe des Tools zur EDS-Hardware-Installation unter http://www.rockwellautomation.com/resources/eds/.

   Berücksichtigen Sie Ihre 1752 SmartGuard-Steuerung und die POINT Guard I/O-Module.

2. Öffnen Sie in der RSLinx-Software das Fenster „RSWho“, und wählen Sie den SmartGuard-Treiber aus.

   RSWho durchsucht das DeviceNet-Netzwerk, das an der SmartGuard-Steuerung angeschlossen ist.

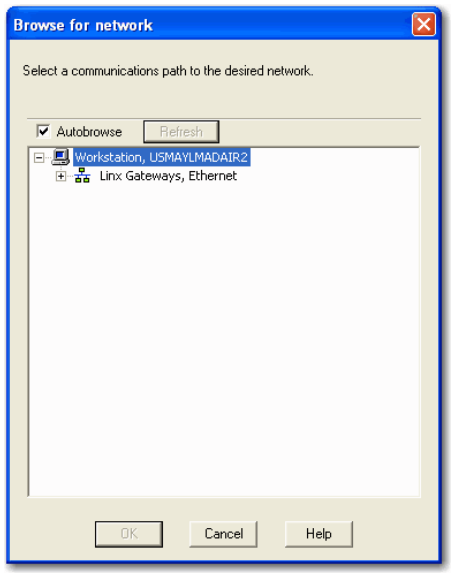
In diesem Beispiel sind zwei POINT Guard I/O-Module an der SmartGuard-Steuerung angeschlossen.



Wenn die Netzknoten im DeviceNet-Netzwerk von der RSLinx-Software erkannt werden, findet auch die Software RSNetWorx for DeviceNet die Netzknoten.

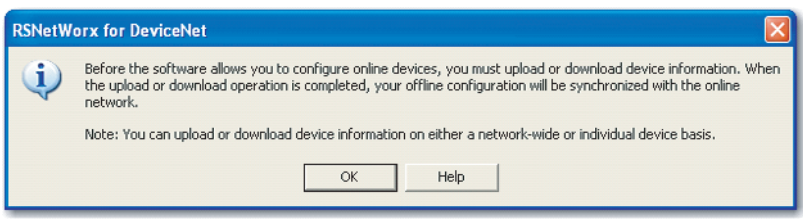
3. Öffnen Sie die Software RSNetWorx for DeviceNet.

4. Wählen Sie im Menü „Networks“ (Netzwerke) die Option „Online“ aus.



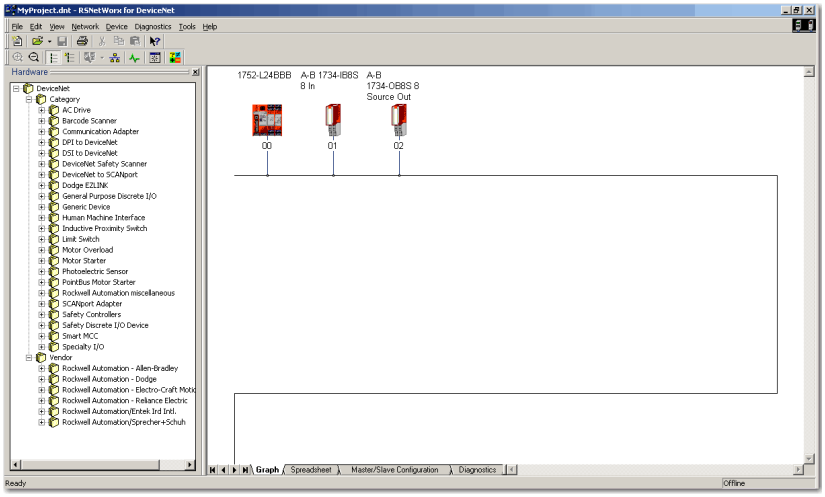
5. Wählen Sie den SmartGuard-Treiber aus, und klicken Sie auf OK.

Das folgende Dialogfenster wird angezeigt.



6. Klicken Sie auf OK.

   Die Software RSNetWorx for DeviceNet findet die SmartGuard- **und** POINT Guard I/O-Module im DeviceNet-Netzwerk.



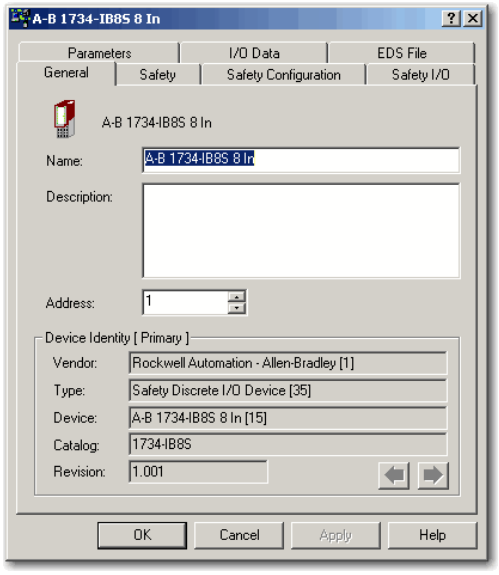
7. Klicken Sie erneut auf das Online-Symbol, um den Offline-Modus zu aktivieren.

Einrichten der Sicherheitskonfiguration

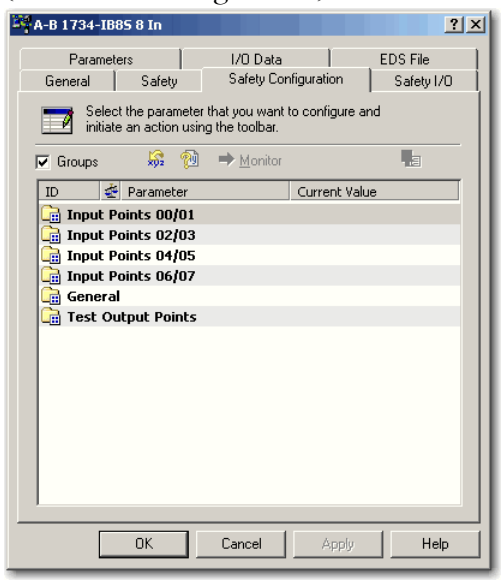
Gehen Sie zum Einrichten der Registerkarte „Safety Configuration“ (Sicherheitskonfiguration) wie folgt vor.

Arbeiten mit Eingängen

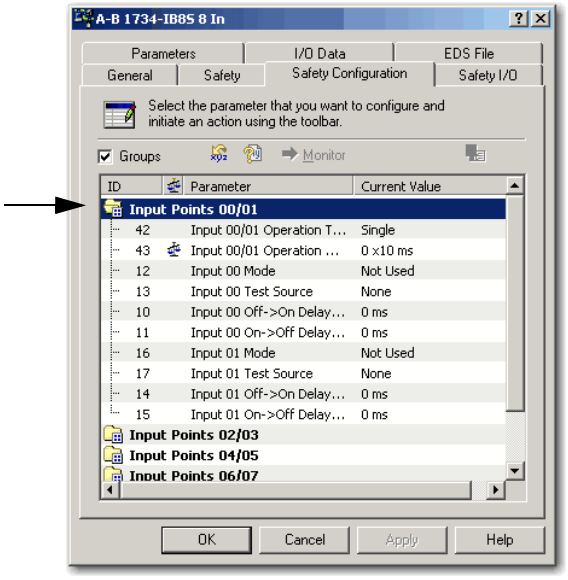
1. Doppelklicken Sie auf das POINT Guard I/O-Modul, um das Dialogfeld „Properties“ (Eigenschaften) zu öffnen.



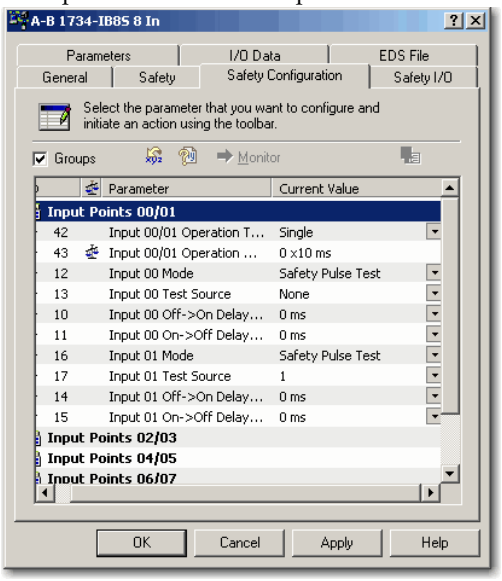
2. Klicken Sie auf die Registerkarte „Safety Configuration“ (Sicherheitskonfiguration).



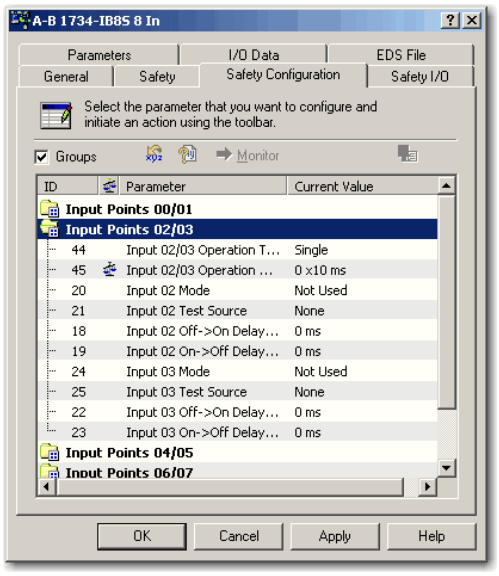
3. Doppelklicken Sie auf die Eingangspunkte 00/01. Beachten Sie, dass es sich bei den Eingängen 00 und 01 um die Not-Halt-Drucktasten handelt.



4. Bearbeiten Sie die Parameter, damit die Kanäle von den Testquellen 0 und 1 Impulstests unterzogen werden.

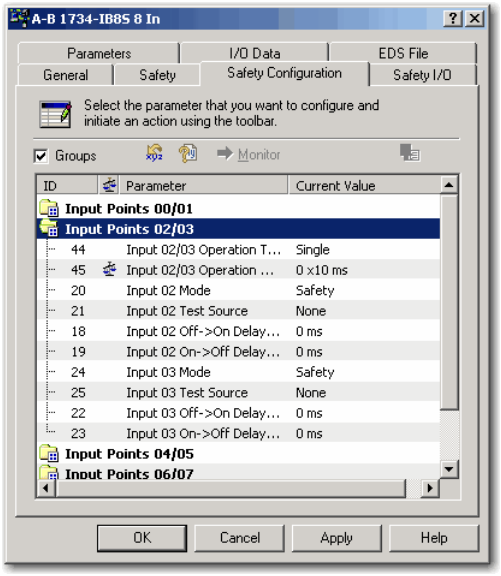


5. Doppelklicken Sie auf die Eingangspunkte 00/01, um diese zu minimieren, und doppelklicken Sie auf die Eingangspunkte 02/03, um diese zu erweitern.



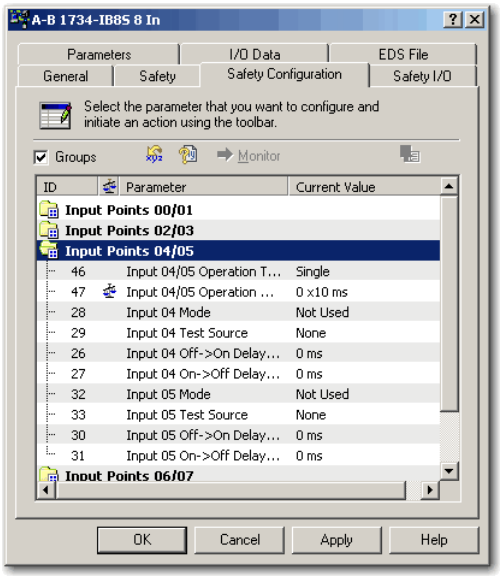
Beachten Sie Folgendes:

- Das Lichtgitter ist an die Eingänge 02 und 03 angeschlossen.
- GuardShield führt Impulstests für OSSD1 und OSSD2 aus, sodass diese Eingänge als Sicherheitseingänge konfiguriert werden.



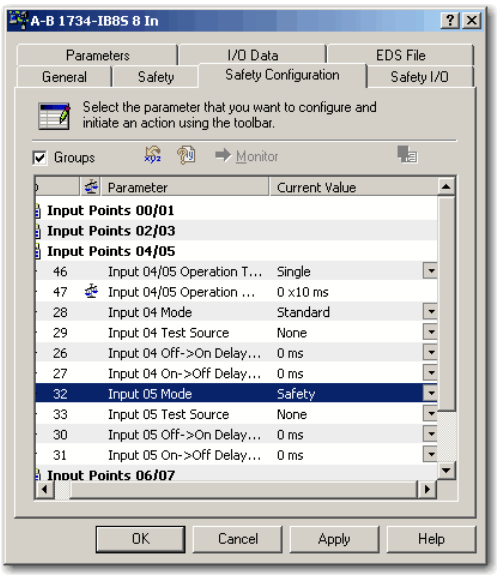
6. Doppelklicken Sie auf die Eingangspunkte 02/03, um diese zu minimieren.

7. Doppelklicken Sie auf die Eingangspunkte 04/05, um diese zu erweitern.



8. Fügen Sie dem Eingang 04 den Rückstellknopf hinzu, und definieren Sie diesen als Standardeingang, da er nicht unbedingt ein Sicherheitseingang sein muss.

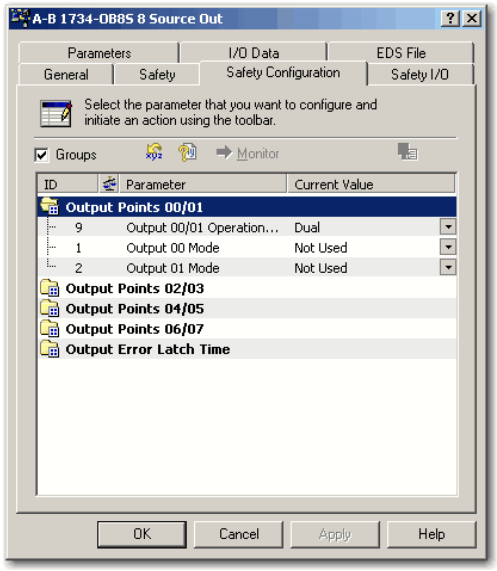
9. Fügen Sie Eingang 05 den AUX-Rückführungsschaltkreis für redundante Sicherheitsschütze hinzu, sodass dieser zu einem Sicherheitseingang wird, da er keinen Impulstests unterzogen wird.



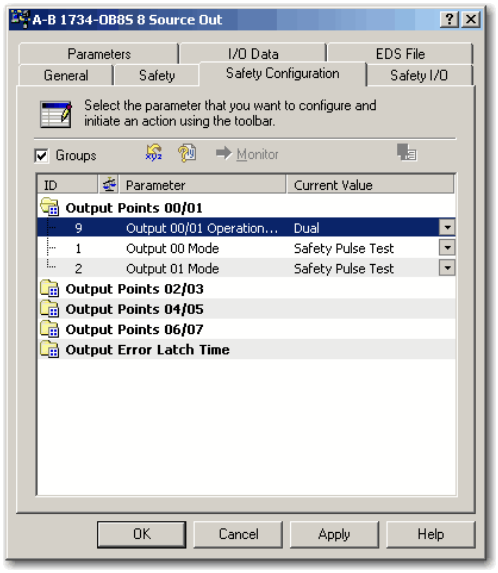
10. Doppelklicken Sie auf die Eingangspunkte 04/05, um diese zu minimieren.

Arbeiten mit Ausgängen

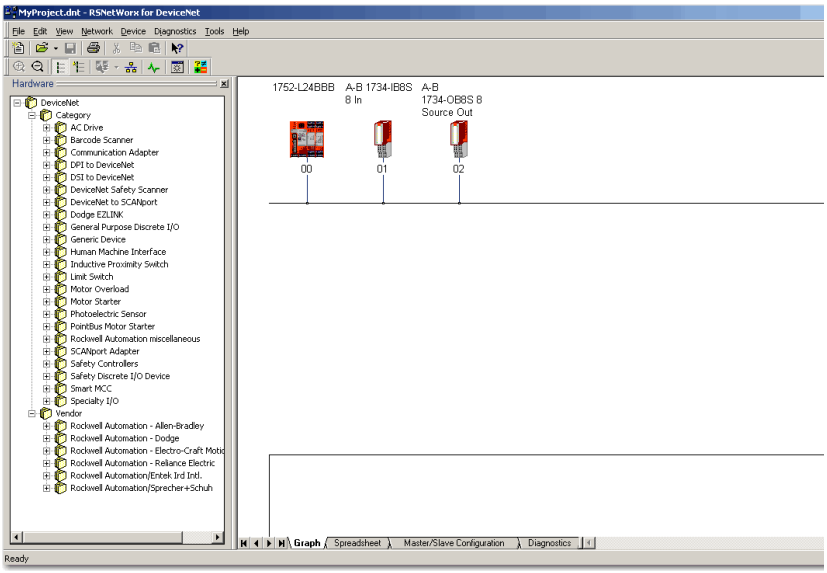
1. Doppelklicken Sie auf die Ausgangspunkte 00/01, um diese zu erweitern. Beachten Sie, dass die Sicherheitsschütze an den Ausgängen 00 und 01 angeschlossen sind.



2. Konfigurieren Sie diese als Sicherheitsimpulstest.



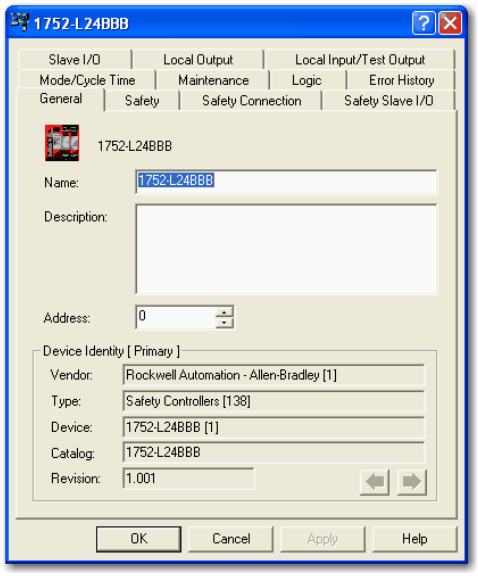
3. Klicken Sie auf „Apply“ (Übernehmen) und OK, um zum Hauptdialogfeld in der Software RSNetWorx for DeviceNet zurückzukehren.



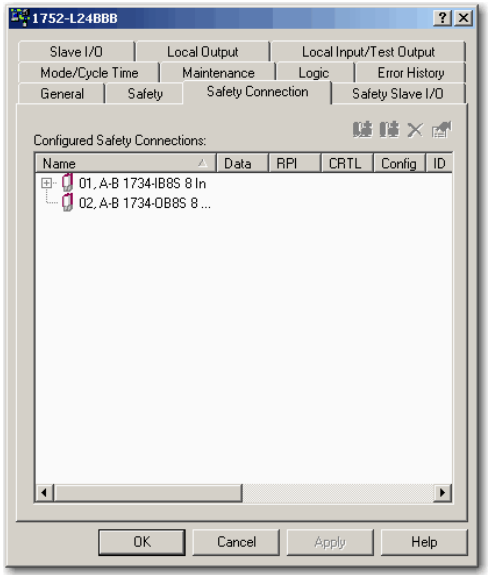
Konfigurieren Sie die Eingangs- und Ausgangsverbindungen der SmartGuard-Steuerung

Gehen Sie wie folgt vor, um die Eingangs- und Ausgangsverbindungen der SmartGuard-Steuerung zu konfigurieren.

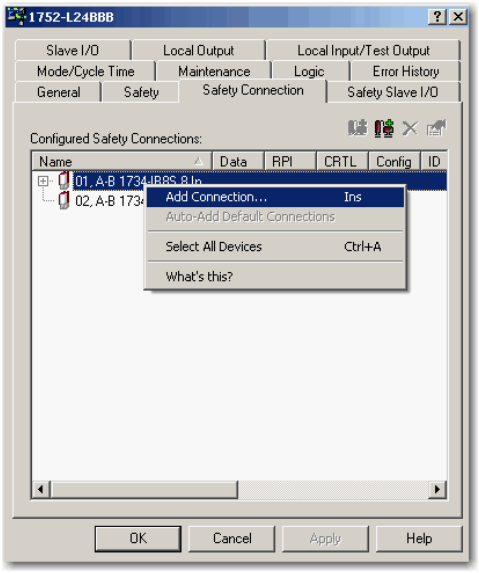
1. Klicken Sie in der Software RSNetWorx for DeviceNet mit der rechten Maustaste auf die SmartGuard-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.



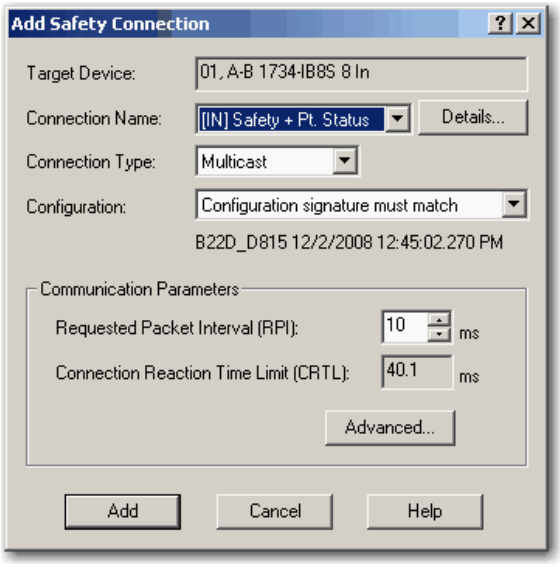
2. Klicken Sie auf die Registerkarte „Safety Connection“ (Sicherheitsverbindung), um eine Liste aller Sicherheits-E/A-Module anzuzeigen, die sich momentan in Ihrem Projekt befinden.



3. Klicken Sie mit der rechten Maustaste auf das POINT Guard I/O-Modul, und wählen Sie „Add Connection“ (Verbindung hinzufügen) aus.



Das Dialogfeld „Add Safety Connection“ (Sicherheitsverbindung hinzufügen) wird angezeigt.



Sie können für die Ein- und Ausgänge einzelne Sicherheitsverbindungen hinzufügen. Die SmartGuard 600-Steuerung kann bis zu 32 Verbindungen aufweisen.

4. Wählen Sie zum Hinzufügen einer Sicherheitsverbindung im Pulldown-Menü „Connection Name“ (Name der Verbindung) eine dieser Optionen aus.

	Auswahl	Beschreibung
1734-IB8S	[IN] Safety	Steuerung der Sicherheitseingänge
	[IN] Safety + Combined Status[a] – Muting	• Steuerung der Sicherheitseingänge • Status für ein Bit für alle Eingänge • Muting-Status ist verfügbar
	[IN] Safety + Pt. Status	• Steuerung der Sicherheitseingänge • Individueller Status jedes Eingangspunkts
	[IN] Safety + Pt. Status – Muting	• Steuerung der Sicherheitseingänge • Individueller Status jedes Eingangspunkts • Muting-Status ist verfügbar
	[IN] Safety + Pt. Status – Muting – Test Output	• Steuerung der Sicherheitseingänge • Individueller Status jedes Eingangspunkts • Muting-Status ist verfügbar • Testausgangsstatus ist verfügbar
	[OUT] Test	Steuerung der Testausgänge
1734-OB8S	[IN] Safety Monitor – Combined Status – Power	• Überwachung der Sicherheitsausgänge • Status für ein Bit für alle Ausgänge • Stromstatus ist verfügbar
	[IN] Safety Output Status	• Individueller Status jedes Ausgangspunkts
	[IN] Safety Output Status + Monitor	• Individueller Status jedes Ausgangspunkts • Überwachung der Sicherheitsausgänge
	[OUT] Safety	Steuerung der Sicherheitsausgänge

a. Die meisten Eingangsverbindungen verwenden den kombinierten Status.

Je mehr Status-Informationen gelesen werden, desto größer sind die Datenpakete.

5. Wählen Sie für dieses Beispiel im Pulldown-Menü „Connection Type“ (Verbindungstyp) die Option „Multicast“ aus.

6. Wählen Sie für dieses Beispiel im Pulldown-Menü „Configuration“ (Konfiguration) die Option „Configuration signature must match“ (Konfigurationssignatur muss übereinstimmen) aus.

7. Geben Sie in das Feld „Requested Packet Interval (RPI)“ (Angefordertes Paketintervall (RPI)) den Wert 10 ms ein.

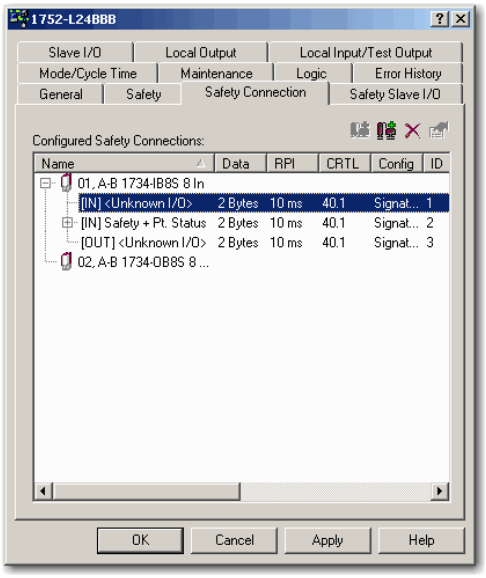
8. Geben Sie in das Feld „Connection Reaction Time Limit (CRTL)“ (Grenzwert für Verbindungsreaktionszeit) den Wert 40,1 ms ein.

9. Klicken Sie auf „Add“ (Hinzufügen).

   Auf diese Weise wird die Datenpaketgröße für die normale Kommunikation begrenzt. Wenn beim Auftreten eines Fehlers ein detaillierter Status erforderlich ist, können diese Daten explizit über MSG-Befehle gelesen werden.

10. Wiederholen Sie die Schritte 3–9 für jede Verbindung. Vergewissern Sie sich dabei, dass Sie die Eingangs- und Ausgangsverbindungen zuordnen.

    Beachten Sie, dass die Verbindungen für das 1734-IB8S-Modul 2 Byte aufweisen. Wenn Sie einen einzelnen Punktstatus ausgewählt haben, würde die Eingangsverbindung 5 Byte aufweisen.



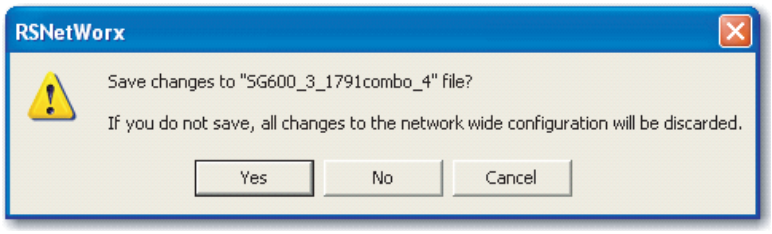
11. Klicken Sie auf „Apply“ (Übernehmen).

Weitere Informationen hierzu finden Sie in der Publikation 1752-UM001, Steuerung SmartGuard 600 – Benutzerhandbuch, und in der Publikation 1752-RM001, SmartGuard 600-Steuerungen – Sicherheitsreferenzhandbuch.

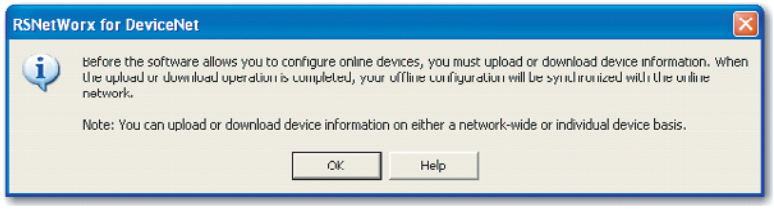
Abschließen der Konfiguration der SmartGuard-Steuerung

1. Klicken Sie im Dialogfeld „1752-L24BBB“ auf „Apply“ (Übernehmen) und anschließend auf OK, um die Verbindung zu akzeptieren.

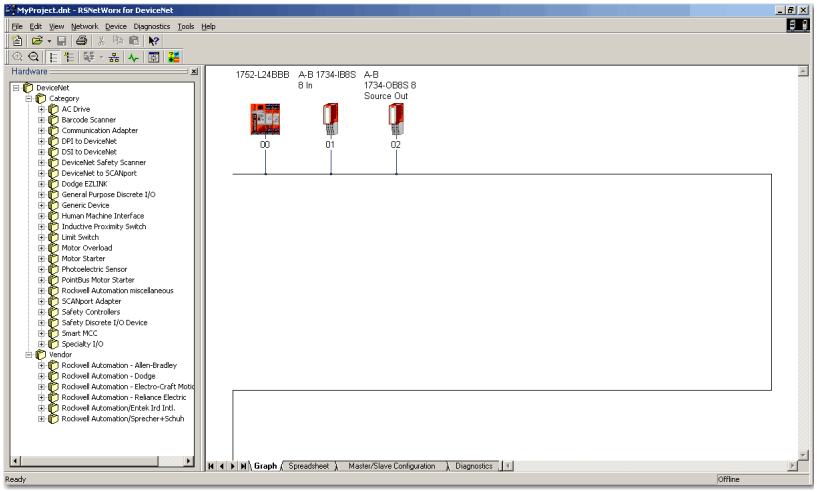
2. Versetzen Sie die Software RSNetWorx for DeviceNet wieder in den Online-Modus.
   a. Wenn dieses Dialogfeld angezeigt wird, klicken Sie auf „Yes“ (Ja), um die Änderungen zu speichern.



   b. Klicken Sie zum Hoch- oder Herunterladen von Gerätedaten auf OK.



Nach dem Durchsuchen werden folgende Netzknoten angezeigt.



Speichern und Herunterladen der Modulkonfiguration

Es wird empfohlen, Ihre Arbeit nach der Konfiguration eines Moduls zu speichern.

Wenn nach dem Herunterladen des Programms die Statusanzeigen MS und NS am POINT Guard I/O-Modul nicht beide konstant grün leuchten, sind eventuell die Verwaltungsrechte verloren gegangen. Die Verwaltungsrechte basieren auf Folgendem:

- POINT Guard I/O-Modulnummer
- POINT Guard I/O-Sicherheitsnetzwerknummer
- SmartGuard-Steckplatznummer
- SmartGuard-Sicherheitsnetzwerknummer
- Pfad von der SmartGuard-Steuerung zum POINT Guard I/O-Modul
- Konfigurationssignatur

Ändert sich einer dieser Werte, wird die Verbindung zwischen der SmartGuard-Steuerung und dem POINT Guard I/O-Modul unterbrochen, und in der RSNetWorks for DeviceNet-Verzeichnisstruktur wird ein gelbes Symbol angezeigt. Weitere Informationen finden Sie in Kapitel 8.

Notizen:

Überlegungen beim Ersetzen der POINT Guard I/O-Module

Inhalt dieses Kapitels

In diesem Kapitel erfahren Sie, was Sie beim Ersetzen von POINT Guard I/O-Modulen berücksichtigen müssen, wenn diese an GuardLogix- oder SmartGuard-Steuerungen angeschlossen sind. Weitere Informationen finden Sie in der Publikation 1756-UM020, GuardLogix-Steuerungen – Benutzerhandbuch, und in der Publikation 1752-UM001, Steuerung SmartGuard 600 – Benutzerhandbuch.

Thema	Seite
Überlegungen beim Ersetzen der POINT Guard I/O-Module	123
Ersetzen eines E/A-Moduls, wenn eine SmartGuard-Steuerung verwendet wird	126
Ersetzen eines E/A-Moduls, wenn eine GuardLogix-Steuerung verwendet wird	130

Überlegungen beim Ersetzen der POINT Guard I/O-Module

Wenn POINT Guard I/O-Module an einer GuardLogix- oder SmartGuard-Steuerung angeschlossen sind, müssen Sie beim Ersetzen der Module Folgendes berücksichtigen.

Das Ersetzen von E/A-Modulen in einem CIP Safety-Netzwerk ist aufgrund der Sicherheitsnetzwerknummer (SNN) weitaus komplizierter als das Ersetzen von Standardgeräten. Die Modulnummer und die SNN ergeben zusammen die Kennung des Sicherheitsmoduls. Sicherheitsgeräte erfordern eine komplexere Kennung, um sicherzustellen, dass doppelte Modulnummern die Kommunikation zwischen den richtigen Sicherheitsgeräten nicht beeinträchtigen.

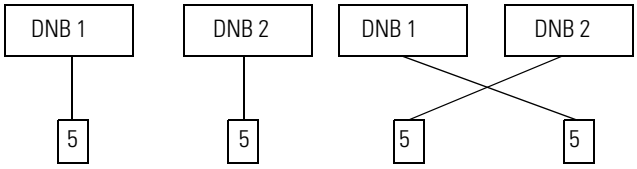
Das folgende einfache Beispiel betrifft ein CompactBlock Guard I/O-Modul in einem DeviceNet-Netzwerk. Ihre Produkte können sich von den Produkten im Beispiel unterscheiden, doch die Funktionsweise ist dieselbe.

BEISPIEL

Das DeviceNet-Netzwerk unterstützt 64 Netzknotennummern. Wenn also in mehreren DeviceNet-Netzwerken 100 Geräte vorliegen, werden mindestens 36 doppelte Netzknotennummern verwendet. Auch wenn sich die doppelten Netzknoten auf verschiedenen DeviceNet-Netzwerken befinden, muss dies in einem Sicherheitssystem dennoch berücksichtigt werden.

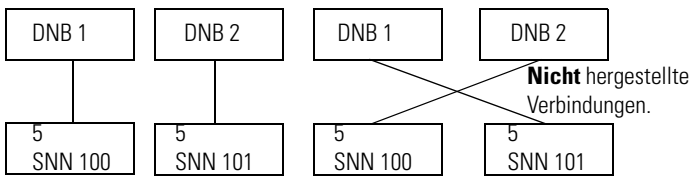
In diesem Beispiel ist der DNB-Scanner 1 an Netzknoten 5 angeschlossen. DNB-Scanner 2 ist an einem anderen Netzknoten mit der Nummer 5 angeschlossen. Wenn die Kabel versehentlich vertauscht werden, könnten die Scanner mit dem falschen Netzknoten 5 kommunizieren.

Beispiel für vertauschte Kabel



Das Szenario mit den vertauschten Kabeln ist für ein Sicherheitssystem nicht akzeptabel. Die SNN garantiert eine eindeutige Identifikation jedes einzelnen Sicherheitsgeräts. Im nächsten Beispiel verfügen alle am DNB-Scanner 1 angeschlossenen Geräte über die SNN 100. Alle am DNB-Scanner 2 angeschlossenen Geräte verfügen über eine SNN von 101. Wenn die Kabel versehentlich vertauscht werden, ändert sich der am DNB-Scanner 1 angeschlossene Netzknoten von 100/5 in 101/5. Der am DNB-Scanner 2 angeschlossene Netzknoten ändert sich von 101/5 in 100/5. Daher werden beim Vertauschen der Kabel **keine** Sicherheitsverbindungen hergestellt.

Beispiel für nicht hergestellte Verbindungen

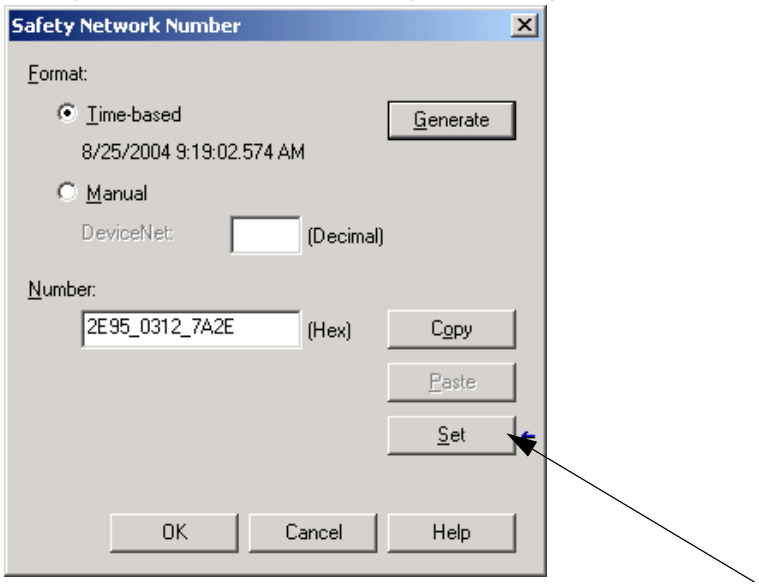


Warum die SNN manuell festgelegt werden muss

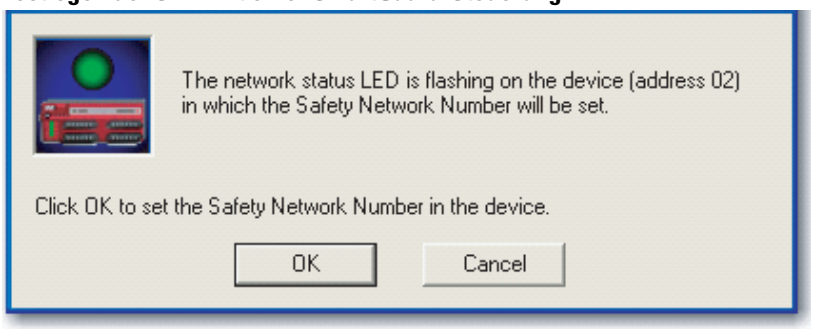
Die Beispiele oben haben gezeigt, wie die SNN verwendet wird, um die Integrität der Sicherheitsverbindung bei betriebsbereitem System zu gewährleisten. Doch die SNN dient auch dazu, die Integrität beim ersten Herunterladen auf das POINT Guard I/O-Modul zu garantieren.

Wenn eine Sicherheitssignatur vorhanden ist, muss das POINT Guard I/O-Modul über eine ordnungsgemäße Kennung aus SNN und Netzknotennummer verfügen, die dem Modul im RSLogix 5000-Projekt entspricht. Erst dann kann es die Konfiguration empfangen. Um die Integrität zu bewahren, **muss** die SNN des Moduls manuell festgelegt werden. Diese manuelle Aktion dient zum „Festlegen“ der Funktion für ein ab Werk konfiguriertes POINT Guard I/O-Modul.

Festlegen der SNN mit einer GuardLogix-Steuerung



Festlegen der SNN mit einer SmartGuard-Steuerung



GuardLogix-Steuerungen im Vergleich zu SmartGuard-Steuerungen

Zwischen den GuardLogix- und SmartGuard-Sicherheitssteuerungen gibt es einen entscheidenden funktionalen Unterschied, der das Ersetzen von Sicherheits-E/A-Modulen betrifft. GuardLogix-Steuerungen speichern die E/A-Modulkonfiguration auf der Platine und können die Konfiguration auf das Austauschmodul herunterladen. SmartGuard-Steuerungen speichern die E/A-Modulkonfiguration nicht. Daher benötigen Sie die Software RSNetWorx for DeviceNet, um die Konfiguration auf das Austauschmodul herunterzuladen.

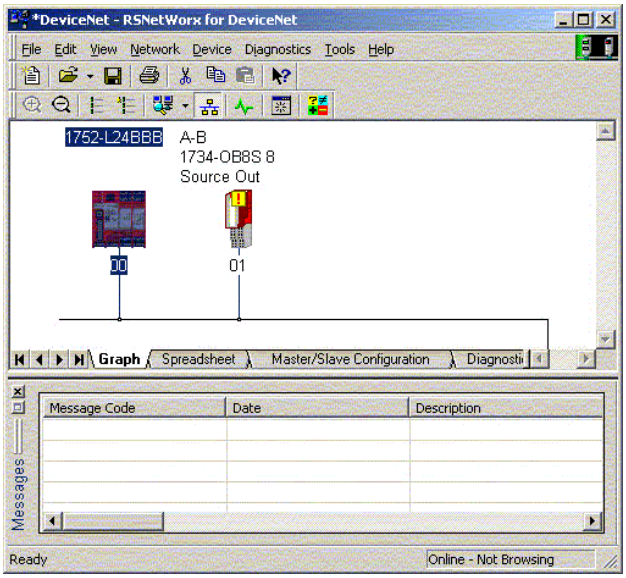
Ersetzen eines E/A-Moduls, wenn eine SmartGuard-Steuerung verwendet wird

Gehen Sie wie folgt vor, um ein E/A-Modul zu ersetzen, wenn Sie eine SmartGuard-Steuerung verwenden.

1. Ersetzen Sie das Modul, und stimmen Sie die Netzknotennummer auf das Originalmodul ab.

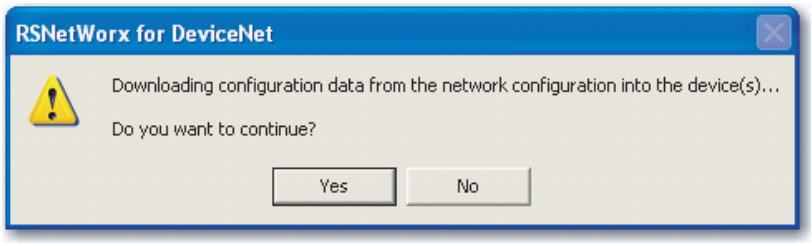
2. Öffnen Sie Ihr Projekt in der Software RSNetWorx for DeviceNet.

   Wenn sich das Austauschmodul im Originalzustand befindet oder eine SNN aufweist, die mit dem ursprünglichen Modul nicht übereinstimmt, wird das Modul mit einem Ausrufezeichen angezeigt.



3. Klicken Sie mit der rechten Maustaste auf das Modul, und wählen Sie „Download to Device“ (Auf Gerät herunterladen) aus.

   Das folgende Dialogfenster wird angezeigt.

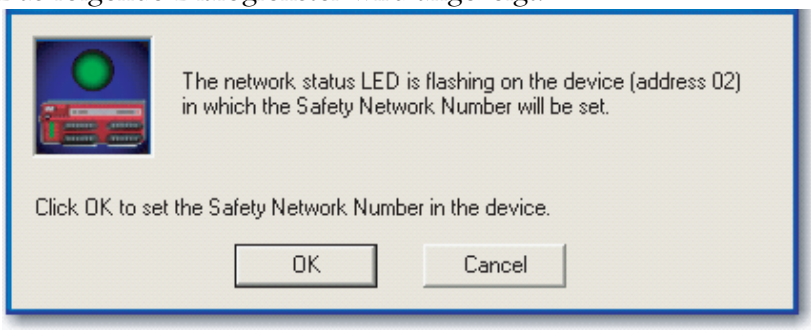


4. Klicken Sie auf „Yes“ (Ja).

   Dieses Dialogfeld wird angezeigt, um Sie darüber zu informieren, dass die SNN des Austauschmoduls nicht mit der SNN in der Software übereinstimmt.

5. Klicken Sie auf „Download“ (Herunterladen), um die SNN auf das Austauschmodul abzustimmen.

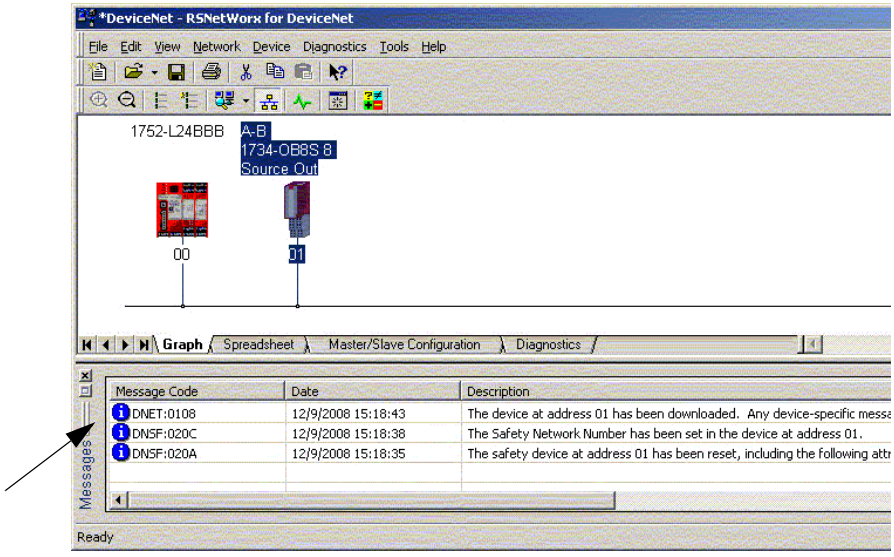
   Das folgende Dialogfenster wird angezeigt.



6. Klicken Sie auf OK.

Dieses Dialogfeld wird angezeigt, um zu bestätigen, dass die SNN festgelegt wurde.

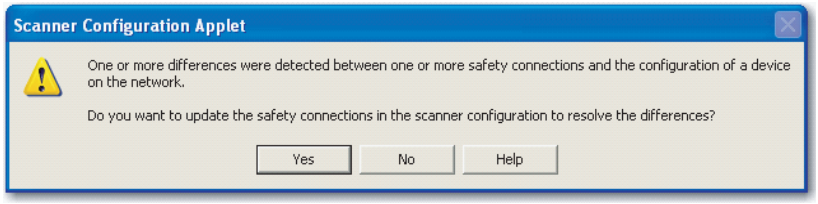
Das Download findet nun statt. Nachdem dieses erfolgreich abgeschlossen wurde, wird in der Hauptansicht des Projekts die folgende Nachricht angezeigt: „The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately.“ (Das Gerät an Adresse *xx* wurde heruntergeladen. Alle gerätespezifischen Nachrichten im Zusammenhang mit dem Download-Vorgang werden separat angezeigt.)



Angenommen, es handelt sich hierbei um die richtige Konfiguration aus der ursprünglichen DNT-Datei, dann stimmen SNN und Konfigurationssignatur nun mit der des Originals überein. Wenn bereits eine Verbindung mit der SmartGuard-Steuerung besteht, wird eine Verbindung hergestellt. Die SmartGuard-Steuerung kann im Run-Modus bleiben, um ein Download zum Austauschmodul durchzuführen.

Wenn Sie diese Konfiguration in ein temporäres Setup herunterladen, platzieren Sie das Modul im Netzwerk. So stellt es die Verbindung zur SmartGuard-Steuerung automatisch her.

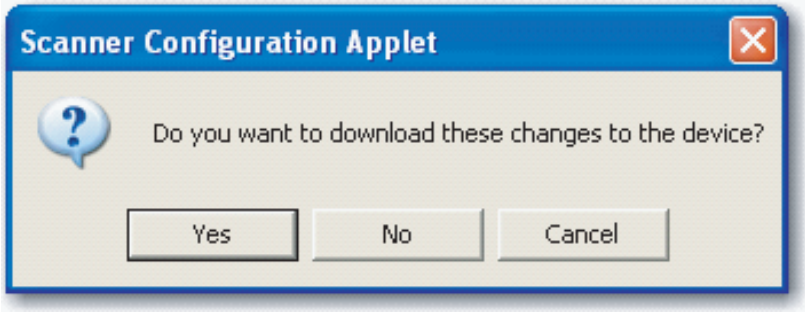
Wenn die auf das Modul heruntergeladene Konfiguration nicht aus der ursprünglichen DNT-Datei stammt, stimmt die Konfigurationssignatur nicht mit dem Original überein. Selbst wenn Sie dieselben Parameter nochmals in einer neuen DNT-Datei erstellen, werden sich die Zeit- und Datumsbestandteile der Signatur unterscheiden, sodass die Verbindung zur SmartGuard-Steuerung nicht hergestellt wird. Wenn dies der Fall ist, klicken Sie für die SmartGuard-Steuerung auf die Registerkarte „Safety Connection“ (Sicherheitsverbindung). In dieser werden Sie darauf aufmerksam gemacht, dass sich die Signatur unterscheidet, und Sie erhalten die Möglichkeit, die neue Signatur abzustimmen. Allerdings sollten Sie das Sicherheitssystem zunächst erneut validieren, da es nicht die ursprüngliche DNT-Datei verwendet.



7. Klicken Sie auf „Yes“ (Ja).

So wird der Run-Modus der SmartGuard-Steuerung deaktiviert.

Es wird das folgende Dialogfeld angezeigt.



8. Klicken Sie auf „Yes“ (Ja), um die neue Verbindungskonfiguration auf die SmartGuard-Steuerung herunterzuladen.

Versetzen Sie die SmartGuard-Steuerung nach dem Download wieder in den Run-Modus. Die Verbindung zum Austauschmodul wird hergestellt.

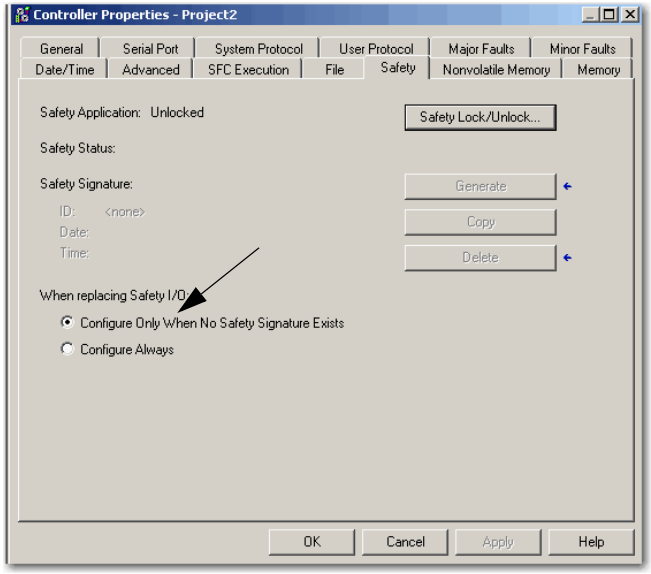
9. Befolgen Sie die Verfahrensvorschriften Ihres Unternehmens, um das ausgetauschte E/A-Modul und das System einem Funktionstest zu unterziehen und das System für die Verwendung freizugeben.

Ersetzen eines E/A-Moduls, wenn eine GuardLogix-Steuerung verwendet wird

Gehen Sie wie folgt vor, um ein E/A-Modul zu ersetzen, wenn Sie eine GuardLogix-Steuerung verwenden.

E/A-Austausch mit aktivierter Option „Configure Only When No Safety Signature Exists“ (Nur konfigurieren, wenn keine Sicherheitssignatur vorhanden ist)

Wählen Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) die Option „Configure Only When No Safety Signature Exists“ (Nur konfigurieren, wenn keine Sicherheitssignatur vorliegt) aus.

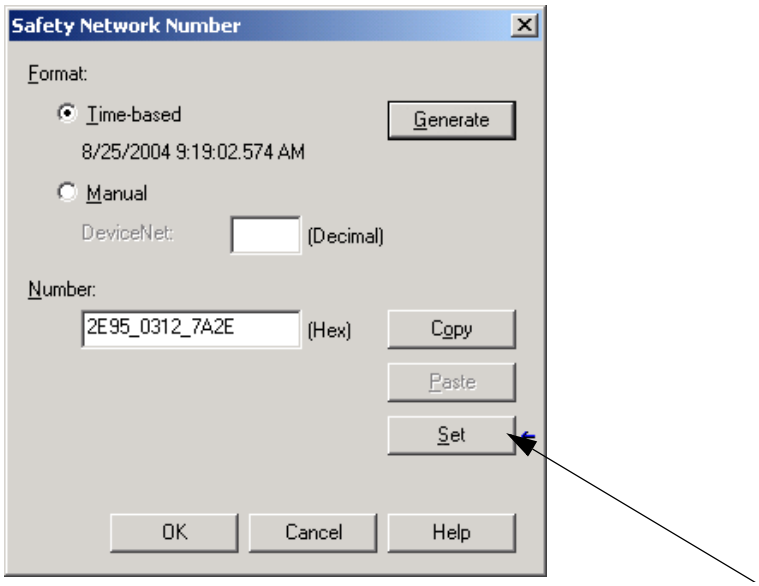


WICHTIG

Wenn Ihre GuardLogix-Steuerung in einer SIL 3-Anwendung verwendet wird, müssen Sie die Option „Configure Only When No Safety Signature Exists“ (Nur konfigurieren, wenn keine Sicherheitssignatur vorliegt) auswählen. Da Sie in SIL 3-Anwendungen über eine Sicherheitssignatur verfügen müssen, stellt diese Option sicher, dass die SNN des E/A-Austauschmoduls mit der der GuardLogix-Steuerung übereinstimmt, bevor eine Verbindung hergestellt wird.

Wenn eine Sicherheitssignatur vorhanden ist, wird durch Klicken auf „Set“ (Festlegen) die richtige SNN vom richtigen GuardLogix-Projekt auf das Austauschmodul heruntergeladen. Einzige Ausnahme wäre, wenn die SNN bereits mit der des Austauschmoduls identisch ist. In diesem Fall wäre keine Maßnahme erforderlich.

Sobald die richtige SNN auf das POINT Guard I/O-Modul heruntergeladen wurde, konfiguriert die GuardLogix-Steuerung das Modul automatisch.



Wenn das Projekt mit der Option „Configure Only When No Safety Signature Exists“ (Nur konfigurieren, wenn keine Sicherheitssignatur vorliegt) konfiguriert wurde, befolgen Sie die entsprechenden Schritte, um ein POINT Guard I/O-Modul basierend auf Ihrem Szenario zu ersetzen.

GuardLogix/ RSLogix 5000-Sicherheits-signatur liegt vor	SNN des Austauschmoduls	Fehler	Erforderliche Aktion
Ja	Werkseinstellungen	SNN nicht festgelegt, Gerät weist Werkseinstellungen auf	Klicken Sie auf „Set“ (Einstellen). Siehe Szenario 1 – Neues Modul weist die Werkseinstellungen auf, und es liegt eine Sicherheitssignatur vor auf Seite 133.
Nein	Werkseinstellungen	Keiner	Keine.

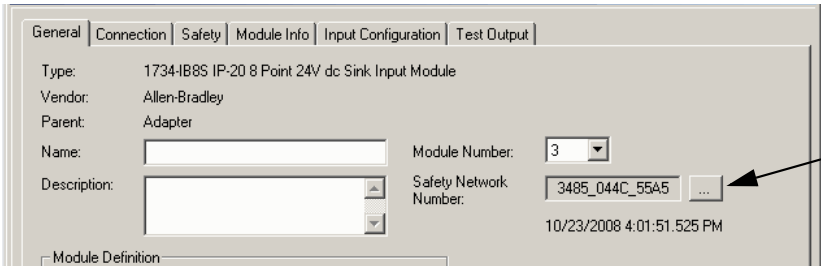
GuardLogix/ RSLogix 5000-Sicherheits-signatur liegt vor	SNN des Austauschmoduls	Fehler	Erforderliche Aktion
Ja oder nein	Mit Original identisch	Keiner	Keine.
Ja	Anders als Original	SNN stimmt nicht überein SNN nicht festgelegt, Gerät weist Werkseinstellungen auf	1. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen). 2. Klicken Sie auf „Set“ (Einstellen). Siehe Szenario 2 – Die SNN des neuen Moduls unterscheidet sich vom Original, und es liegt eine Sicherheitssignatur vor auf Seite 134.
Nein	Anders als Original	SNN stimmt nicht überein	Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen). Siehe Szenario 3 – Die SNN des neuen Moduls unterscheidet sich vom Original, und es liegt keine Sicherheitssignatur vor auf Seite 136.

Szenario 1 – Neues Modul weist die Werkseinstellungen auf, und es liegt eine Sicherheitssignatur vor

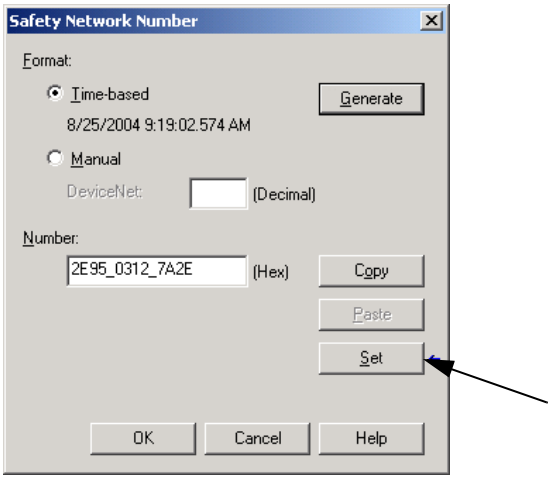
1. Bauen Sie das alte E/A-Modul aus, und installieren Sie das neue Modul.

2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul, und wählen Sie „Properties“ (Eigenschaften) aus.

3. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.

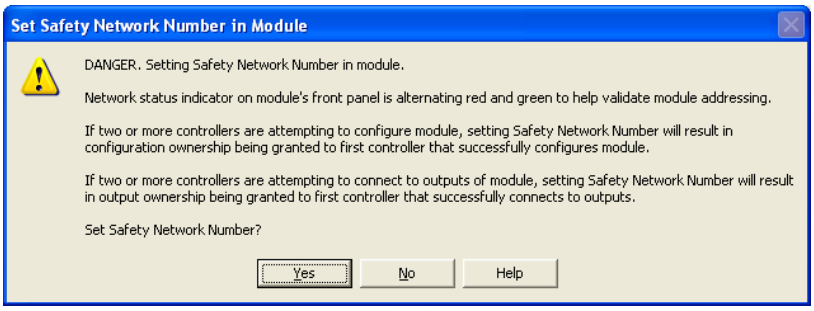


4. Klicken Sie auf „Set“ (Einstellen).



Das Bestätigungsdialogfeld „Set Safety Network Number in Module“ (Sicherheitsnetzwerknummer im Modul einstellen) wird angezeigt.

5. Vergewissern Sie sich, dass die Statusanzeige für den Netzwerkstatus (NS) am richtigen Modul abwechselnd rot und grün aufleuchtet, bevor Sie auf „Yes“ (Ja) klicken, um die SNN festzulegen und das Austauschmodul zu akzeptieren.



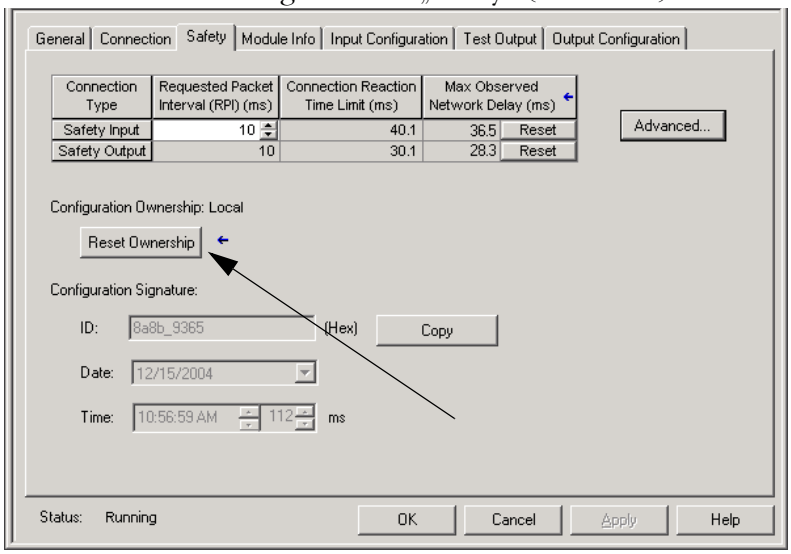
6. Befolgen Sie die Vorschriften Ihres Unternehmens, um das ausgetauschte E/A-Modul und das System einem Funktionstest zu unterziehen und das System für die Verwendung freizugeben.

Szenario 2 – Die SNN des neuen Moduls unterscheidet sich vom Original, und es liegt eine Sicherheitssignatur vor

1. Bauen Sie das alte E/A-Modul aus, und installieren Sie das neue Modul.

2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul, und wählen Sie „Properties“ (Eigenschaften) aus.

3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).

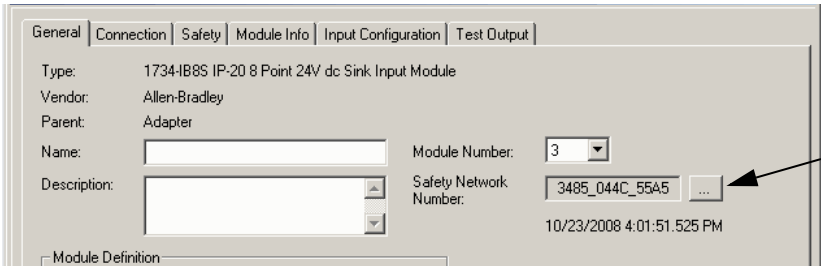


4. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).

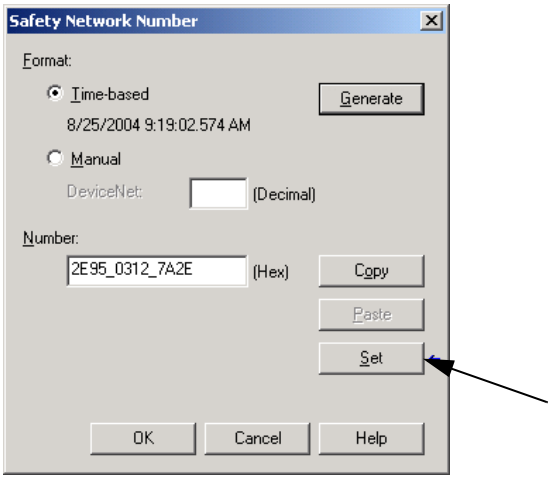
5. Klicken Sie auf OK.

6. Klicken Sie mit der rechten Maustaste auf Ihre GuardLogix-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

7. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.

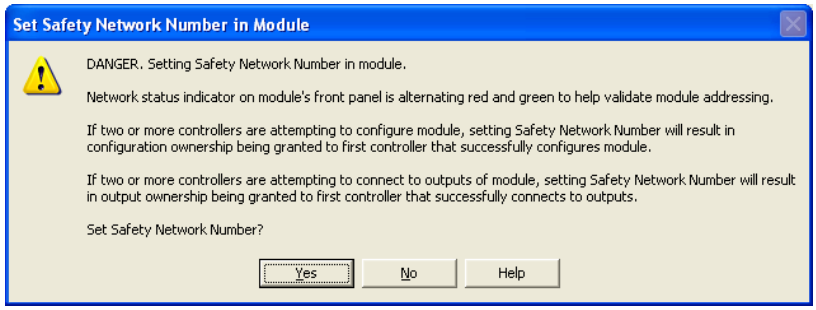


8. Klicken Sie auf „Set“ (Einstellen).



Das Bestätigungsdialogfeld „Set Safety Network Number in Module“ (Sicherheitsnetzwerknummer im Modul einstellen) wird angezeigt.

9. Vergewissern Sie sich, dass die Statusanzeige für den Netzwerkstatus (NS) am richtigen Modul abwechselnd rot und grün aufleuchtet, bevor Sie auf „Yes“ (Ja) klicken, um die SNN festzulegen und das Austauschmodul zu akzeptieren.



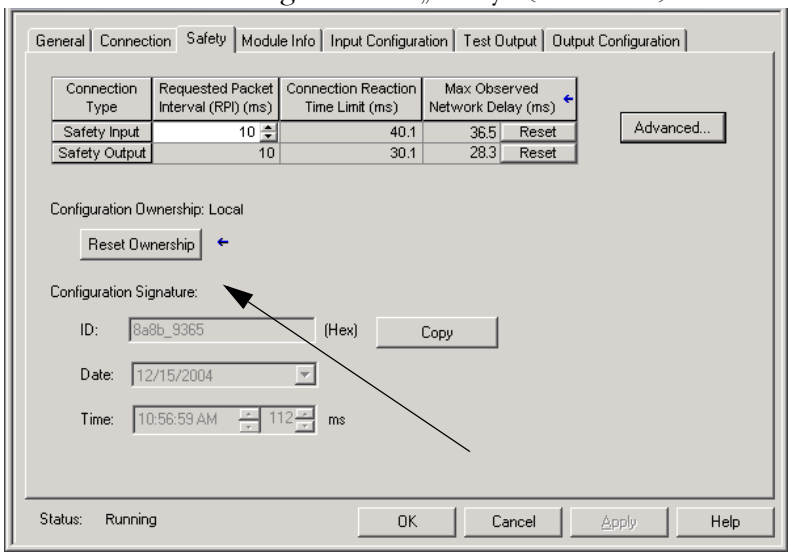
10. Befolgen Sie die Verfahrensvorschriften Ihres Unternehmens, um das ausgetauschte E/A-Modul und das System einem Funktionstest zu unterziehen und das System für die Verwendung freizugeben.

Szenario 3 – Die SNN des neuen Moduls unterscheidet sich vom Original, und es liegt keine Sicherheitssignatur vor

1. Bauen Sie das alte E/A-Modul aus, und installieren Sie das neue Modul.

2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul, und wählen Sie „Properties“ (Eigenschaften) aus.

3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



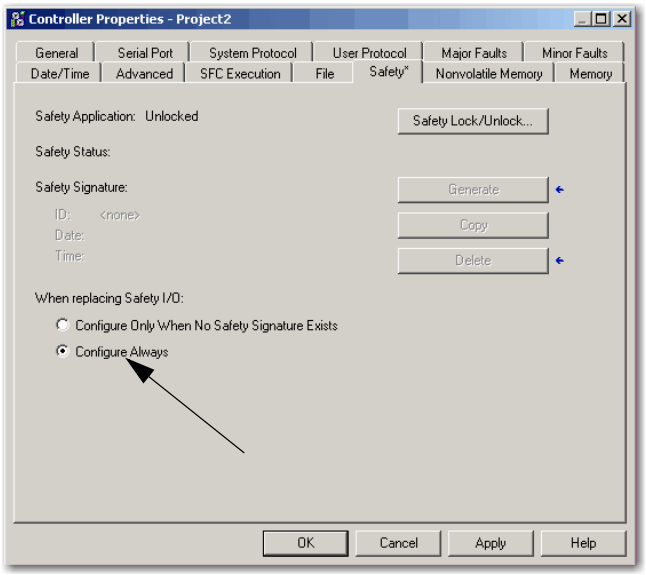
4. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).

5. Klicken Sie auf OK.

6. Befolgen Sie die Verfahrensvorschriften Ihres Unternehmens, um das ausgetauschte E/A-Modul und das System einem Funktionstest zu unterziehen und das System für die Verwendung freizugeben.

E/A-Austausch mit aktivierter Option „Configure Always“ (Immer konfigurieren)

Wählen Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) die Option „Configure Always“ (Immer konfigurieren) aus.



ACHTUNG

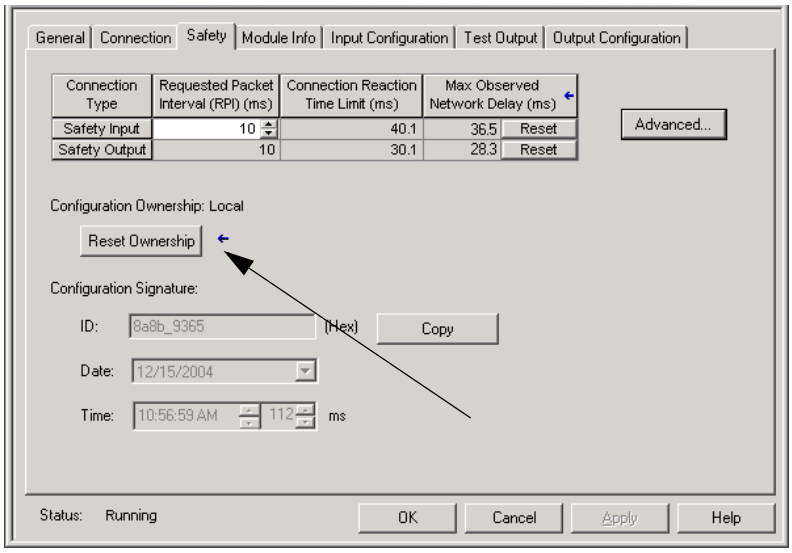
Aktivieren Sie die Option „Configure Always“ (Immer konfigurieren) nur, wenn das gesamte CIP Safety-Steuerungssystem **nicht** erforderlich ist, um das SIL 3-Verhalten während des Austauschs und der Funktionstests eines Moduls aufrechtzuerhalten.

Wenn die Funktion „Configure Always“ (Immer konfigurieren) in der Software RSLogix 5000 aktiviert ist, überprüft die Steuerung automatisch, ob ein Austauschmodul vorliegt, das alle der folgenden Bedingungen erfüllt. Anschließend stellt sie automatisch eine Verbindung zu diesem Modul her:

- Die Steuerung verfügt über Konfigurationsdaten für ein kompatibles Modul an dieser Netzwerkadresse.
- Das Modul weist die Werkseinstellungen auf oder verfügt über eine SNN, die mit der Konfiguration übereinstimmt.

Auch wenn die Chancen gering sind, kann dadurch dennoch die falsche Steuerung die Verwaltungsrechte für das Austauschmodul übernehmen. Daher müssen Sie nach dem Herunterladen Tests ausführen, um sicherzustellen, dass dies nicht geschehen ist.

Bei Modulen mit unterschiedlichen SNNs wird durch Klicken auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen) das Modul auf die Werkseinstellungen zurückgesetzt. Sobald das Modul die Werkseinstellungen aufweist, müssen Sie nichts mehr unternehmen, damit die GuardLogix-Steuerung die Verwaltungsrechte des Moduls übernimmt.



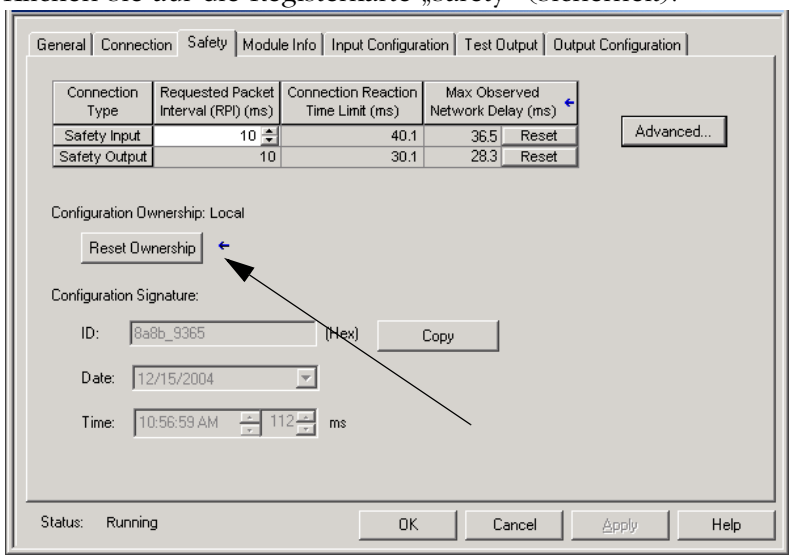
Wenn das Projekt mit der Option „Configure Always“ (Immer konfigurieren) konfiguriert wurde, befolgen Sie die entsprechenden Schritte, um ein POINT Guard I/O-Modul basierend auf Ihrem Szenario zu ersetzen.

GuardLogix/ RSLogix 5000-Sicherheits-signatur liegt vor	SNN des Austauschmoduls	Fehler	Erforderliche Aktion
Ja oder nein	Werkseinstellungen	Keiner	Keine.
Ja oder nein	Mit Original identisch	Keiner	Keine.
Ja oder nein	Anders als Original	SNN stimmt nicht überein	Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen). Gehen Sie wie unten beschrieben vor.

1. Bauen Sie das alte E/A-Modul aus, und installieren Sie das neue Modul.

2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul, und wählen Sie „Properties“ (Eigenschaften) aus.

3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



4. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).

5. Klicken Sie auf OK.

6. Befolgen Sie die Verfahrensvorschriften Ihres Unternehmens, um das ausgetauschte E/A-Modul und das System einem Funktionstest zu unterziehen und das System für die Verwendung freizugeben.

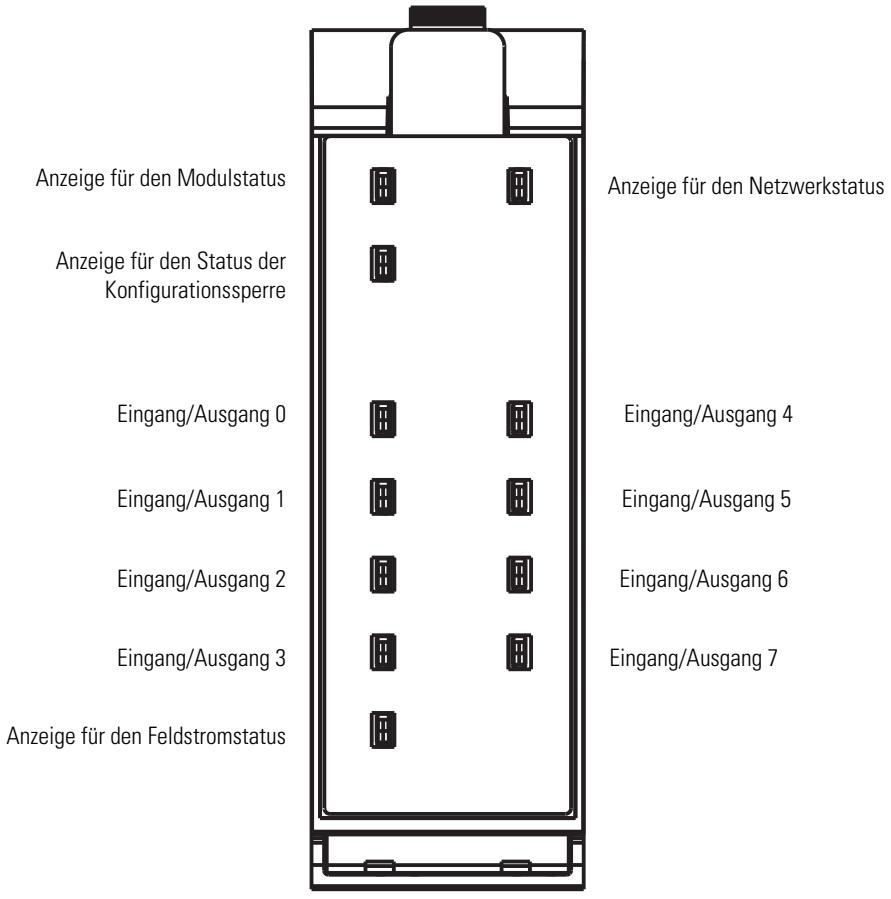
Statusanzeigen

Einleitung

Beachten Sie bei Bedarf die folgenden Statusanzeigen.

Thema	Seite
Modulstatus	142
Netzwerkstatus	142
Konfigurationssperre	143
Spannungsversorgung	143
Status des sicheren Eingangs (1734-IB8S-Modul)	143
Status des sicheren Ausgangs (1734-OB8S-Modul)	144

Positionen der Statusanzeigen



Modulstatus

Anzeige	Status	Beschreibung	Empfohlene Maßnahme
MS	Aus	Es liegt keine Spannung am Modul an.	Legen Sie an diesem Anschluss Spannung an.
	Dauerhaft grün	Das Modul arbeitet normal.	Keine.
	Dauerhaft rot	Das Modul hat eine nicht korrigierbare Störung erkannt.	Schalten Sie das Modul aus und wieder ein. Falls das Problem weiterhin besteht, tauschen Sie das Modul aus.
	Grün blinkend	Das Gerät befindet sich im Leerlauf oder im Standby.	Konfigurieren Sie das Modul, und stellen Sie eine Verbindung her.
	Rot blinkend	Das Modul hat einen korrigierbaren Fehler erkannt.	Schalten Sie das Modul aus und wieder ein, oder setzen Sie das Modul zurück.
		Vom Anwender eingeleitetes Firmware-Update wird ausgeführt.	Warten Sie, bis das Firmware-Update abgeschlossen ist.
	Rot und grün blinkend	Modul ist nicht konfiguriert.	Konfigurieren Sie das Modul neu. Weitere Informationen finden Sie in der Tabelle zur Netzwerkstatusanzeige.
		Das Modul führt die Einschaltdiagnose durch.	Warten Sie, bis das Modul seine Einschaltdiagnose abgeschlossen hat.

Netzwerkstatus

Anzeige	Status	Beschreibung	Empfohlene Maßnahme
NS	Aus	Das Modul ist online mit dem Netzwerk, und es liegt keine Spannung an.	Stellen Sie sicher, dass Ihr Netzwerk ordnungsgemäß funktioniert.
	Grün blinkend	Modul ist online, es wurden keine Verbindungen hergestellt.	Überprüfen Sie Ihr Netzwerk und die Modulkonfiguration.
		Das Modul hat die Kommunikationsgeschwindigkeit des Netzwerks erkannt, doch es wurden keine Verbindungen hergestellt.	
	Dauerhaft grün	Modul ist online, es wurden Verbindungen hergestellt Das Modul arbeitet normal.	Keine.
	Rot blinkend	Zeitabschaltung bei mindestens einer E/A-Verbindung.	Überprüfen Sie Ihr Netzwerk und die Modulkonfiguration.
		Vom Anwender eingeleitetes Firmware-Update wird ausgeführt.	Warten Sie, bis das Firmware-Update abgeschlossen ist.
	Dauerhaft rot	Kritischer Verbindungsfehler. Das Modul hat einen Fehler erkannt, der die Kommunikation im Netzwerk verhindert, wie beispielsweise eine doppelte Netzknotenadresse.	Schalten Sie das Modul aus und wieder ein. Überprüfen Sie die Netzknotenadresse.

Konfigurationssperre

Anzeige	Status	Beschreibung	Empfohlene Maßnahme
LK[a]	Aus	Keine Konfiguration oder Konfiguration durch eine GuardLogix-Steuerung.	Überprüfen Sie die Konfiguration mit einem Tool zur Netzwerkkonfiguration, wie z. B. die RSNetWorx-Software.
		Ungültige Konfigurationsdaten.	
	Dauerhaft gelb	Gesperrt.	Keine.
		Gültige Konfiguration, durch ein Tool zur Netzwerkkonfiguration gesperrt, wie z. B. die RSNetWorx-Software.	
	Gelb blinkend	Nicht gesperrt.	Keine.
		Gültige Konfiguration mit einem Tool zur Netzwerkkonfiguration, wie z. B. die RSNetWorx-Software.	

a. Nicht zutreffend, wenn mit den GuardLogix-Steuerungen verwendet.

Spannungsversorgung

Anzeige	Status	Beschreibung	Empfohlene Maßnahme
PWR	Aus	Es liegt keine Feldspannung an.	Legen Sie Feldspannung an.
	Grün	Normale Bedingung, Feldspannung liegt an und liegt innerhalb der Spezifikationen.	Keine.
	Gelb	Feldspannung außerhalb der Spezifikationen.	Überprüfen Sie Ihre Anschlüsse, Verdrahtung und Spannungen.

Status des sicheren Eingangs (1734-IB8S-Modul)

Anzeige	Status	Beschreibung	Empfohlene Maßnahme
0–7	Aus	Sicherheitseingang ist ausgeschaltet, oder Modul wird konfiguriert.	Schalten Sie den Sicherheitseingang ein, oder konfigurieren Sie den Kanal ggf. neu.
	Gelb	Sicherheitseingang ist eingeschaltet.	Keine.
	Rot	In der externen Verdrahtung bzw. in der Eingangsschaltung wurde eine Störung erkannt.	Überprüfen Sie Konfiguration, Feldverdrahtung und Geräte. Wenn Sie kein Problem feststellen können, muss das Modul ausgetauscht werden.
	Rot blinkend	In der Partner-Eingangsschaltung einer Doppeleingangskonfiguration wurde eine Störung erkannt.	Überprüfen Sie die Feldverdrahtung sowie die Konfiguration für die Partnerschaltung. Wenn Sie kein Problem feststellen können, muss das Modul ausgetauscht werden.

Status des sicheren Ausgangs (1734-OB8S-Modul)

Anzeige	Status	Beschreibung	Empfohlene Maßnahme
0–7	Aus	Sicherheitsausgang ist ausgeschaltet oder Modul wird konfiguriert.	Schalten Sie den Sicherheitsausgang ein, oder konfigurieren Sie den Kanal ggf. neu.
	Gelb	Sicherheitsausgang ist eingeschaltet.	Keine.
	Rot	In der Ausgangsschaltung wurde eine Störung erkannt.	Überprüfen Sie die Schaltkreis-Verdrahtung und das Endgerät. Wenn Sie kein Problem feststellen können, muss das Modul ausgetauscht werden.
		Die Tags in einer Konfiguration mit zwei Ausgängen weisen unterschiedliche Werte auf.	Die Programmlogik muss sicherstellen, dass die Tag-Werte identisch sind (AUS oder EIN).
	Rot blinkend	In der Partner-Ausgangsschaltung einer Doppelausgangskonfiguration wurde eine Störung erkannt.	Überprüfen Sie die Schaltkreis-Verdrahtung und das Endgerät des Partners. Wenn Sie kein Problem feststellen können, muss das Modul ausgetauscht werden.

Abrufen des E/A-Diagnosestatus von Modulen in Logix-Systemen

Thema	Seite
Einleitung	145
Nachrichtenbefehle	145

Einleitung

Mithilfe von Nachrichtenbefehlen in einem Logix-System können Sie die Ursache von Eingangspunkt- oder Ausgangspunktfehlern ermitteln.

Nachrichtenbefehle

Wenn die Steuerung einen Fehler an einem Eingangs- oder Ausgangspunkt erkennt, können Sie mithilfe eines Nachrichtenbefehls die Ursache des Fehlers explizit abrufen.

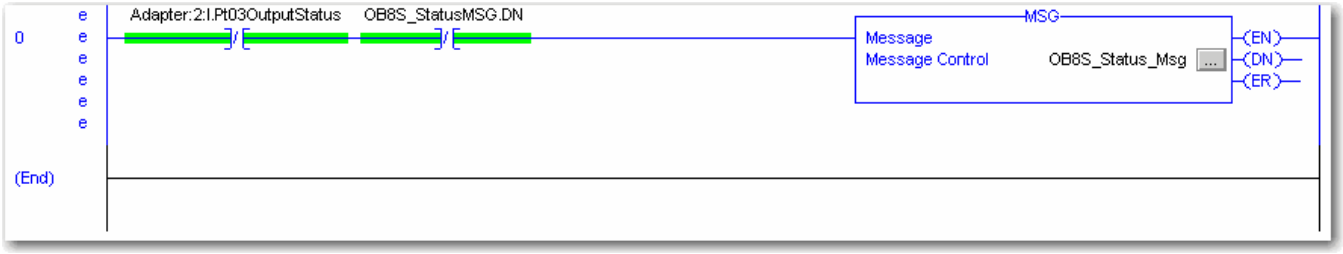
In diesem Beispiel wird ein 1734-OB8S-Modul verwendet, dessen Eingangsstatus so konfiguriert ist, dass der Punktstatus zurückgegeben wird. In der folgenden Tabelle sind die Steuerungs-Tags dargestellt, die Sie für dieses Modul überwachen können.

Adapter:2:I.Pt00OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt01OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt02OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt03OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt04OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt05OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt06OutputStatus	0		Decimal	BOOL	Safety
Adapter:2:I.Pt07OutputStatus	0		Decimal	BOOL	Safety

Verwenden Sie die Bits für den Punktausgangsstatus, um festzustellen ob mindestens einer der Ausgangspunkte am Modul einen Fehler aufweist.

- Wenn ein Status-Bit den Wert 0 (0 = Fehler, 1 = kein Fehler) annimmt, können Sie mit Hilfe des Status-Bits Ihren Nachrichtenbefehl wie folgt konditionieren.
- Platzieren Sie diese Strompfade in der Standard-Task.

In diesem Beispiel einer Kontaktplanlogik wird der Status von Ausgangspunkt 3 überwacht. Dieser Kontaktplanlogik-Strompfad überprüft den Ausgangspunktstatus. Falls ein Fehler erkannt wird (0 = Fehler), wird der Nachrichtenbefehl ausgeführt.

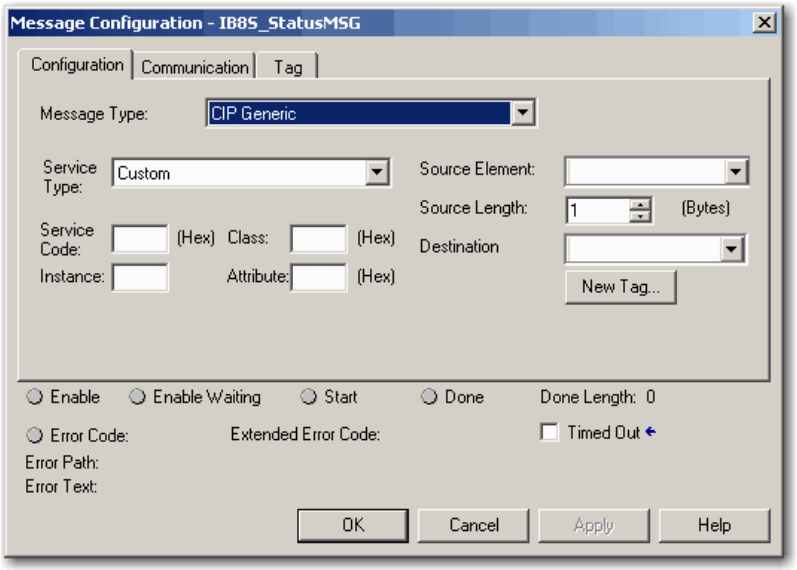


Konfigurieren Sie den Nachrichtenbefehl

Gehen Sie wie folgt vor, um Eingaben im Dialogfeld „Message Configuration“ (Nachrichtenkonfiguration) vorzunehmen.

1. Klicken Sie in der Kontaktplanlogik des Nachrichtenbefehls auf das Symbol ...

2. Geben Sie die entsprechenden Daten für die zu überwachenden Elemente ein.

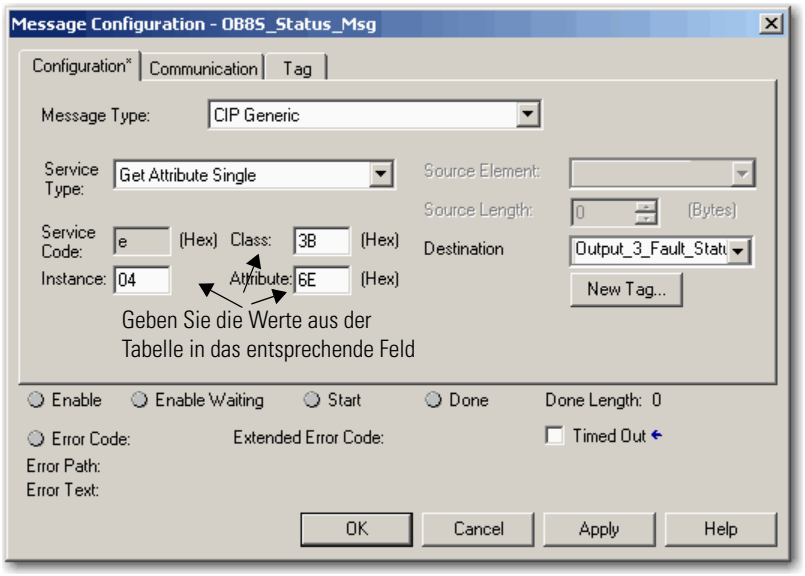


3. Wählen Sie im Pulldown-Menü „Service Type“ (Servicetyp) die Option „Get Attribute Single“ (Abrufen Einzelattribut) aus.

4. Entnehmen Sie abhängig von den zu überwachenden Elementen die Werte der entsprechenden Tabelle.

   Dieses Dialogfeld zeigt die Werte, die Sie eingeben müssen, um die Ursache für den Fehler in Ausgang 3 zu bestimmen.

TIPP Geben Sie für den Wert „Instance" (Instanz) den Eingangs-/Ausgangspunkt plus 1 ein. Im vorliegenden Beispiel entspricht Ausgangspunkt 3 der Instanz 4.



Überwachen eines Sicherheitseingangsstatus

Servicetyp	Funktion	Befehl (hex)					Antwort (hex)
		Service-code	Klassen-ID	Instanz-ID	Attribut-ID	Daten-größe	
Get Attribute Single (Abrufen Einzelattribut)	Liest die Ursache für den Sicherheitseingangsfehler aus, der durch die Instanz-ID (1–8) angegeben wird.	0E	3D	01–08	6E	–	0: Kein Fehler 01: Konfiguration ungültig 02: Fehler externes Testsignal 03: Interner Eingangsfehler 04: Diskrepanzfehler 05: Fehler im anderen zweikanaligen Eingang

Überwachen eines Sicherheitsausgangsstatus

Servicetyp	Funktion	Befehl (hex)					Antwort (hex)
		Servicecode	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Get Attribute Single (Abrufen Einzelattribut)	Liest die Ursache für den Sicherheitsausgangsfehler aus, der durch die Instanz-ID (1–8) angegeben wird.	0E	3B	01–08	6E	–	0: Kein Fehler 01: Konfiguration ungültig 02: Überstrom erkannt 03: Kurzschluss erkannt 04: Fehler Ausgang eingeschaltet 05: Fehler im anderen zweikanaligen Ausgang 06: N. z. 07: N. z. 08: Zweikanalige Verletzung 09: Kurzschluss erkannt am Sicherheitsausgang

Überwachen eines Testausgangsstatus

Servicetyp	Funktion	Befehl (hex)					Antwort (hex)
		Servicecode	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Get Attribute Single (Abrufen Einzelattribut)	Liest die Ursache des Testausgangsfehlers aus, der durch die Instanz-ID (1–4) angegeben wird.	0E	09	01–04	76	–	0 = Kein Fehler 01: Konfiguration ungültig 02: Überlast erkannt 03: Querschluss erkannt 05: Fehler Ausgang eingeschaltet 06: Unterstrom für Muting-Leuchte erkannt

Konfigurieren von Testausgängen für Kommunikationsfehler

Servicetyp	Funktion	Befehl (hex)					Antwort (hex)
		Servicecode	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Festlegen Einzelattribut	Konfiguriert den Testausgang so, dass er nach einem Kommunikationsfehler an einem durch die Instanz-ID angegebenen Ausgang entweder deaktiviert wird oder seinen letzten Zustand hält.	10	09	01–04	05	1 Byte 00: Löschen 01: Halten	-

Versagenswahrscheinlichkeit bei Anforderung (PFD), Versagenswahrscheinlichkeit pro Stunde (PFH) und mittlerer Ausfallabstand (MTBF)

Inhalt dieses Anhangs

Dieser Anhang enthält berechnete Werte für die Versagenswahrscheinlichkeit bei Anforderung, die Versagenswahrscheinlichkeit pro Stunde und den mittleren Ausfallabstand.

Berechnete Werte

Siehe die Tabelle mit den Werten. Referenzinformationen in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

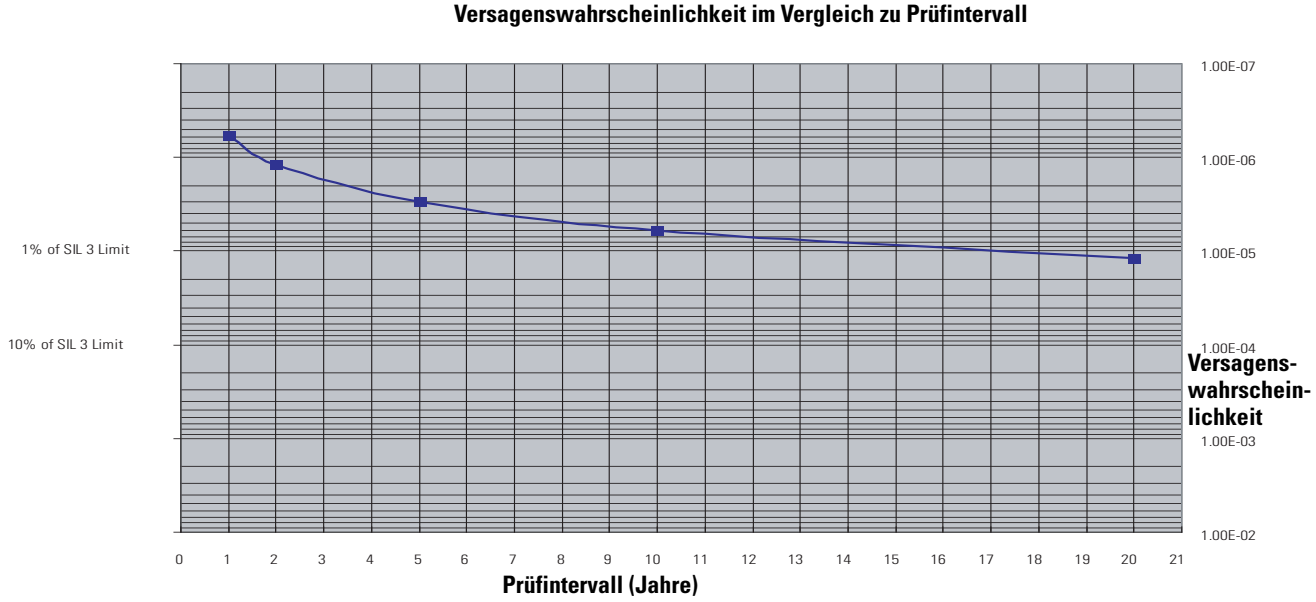
Die berechneten Werte der Versagenswahrscheinlichkeit bei Anforderung und der Versagenswahrscheinlichkeit pro Stunde sind in der Tabelle enthalten und müssen für die Geräte innerhalb des Systems berechnet werden, um der für die Anwendung erforderlichen SIL-Ebene zu entsprechen.

Die Anwender sind für die Einhaltung der folgenden Anforderungen von ISO 13849-1:2008 verantwortlich, um die Leistungsebenen in ihrem Sicherheitssystem beurteilen zu können.

Innerhalb des Intervalls der Bewährungsprüfung muss jedes E/A-Modul auf seine Funktionstüchtigkeit getestet werden. Schalten Sie hierzu jeden Eingangspunkt um, und stellen Sie sicher, dass dieser von der Steuerung erkannt wird.

Darüber hinaus muss jeder Ausgangspunkt einzeln von der Steuerung umgeschaltet werden. Dabei muss der Anwender sicherstellen, dass der Ausgangspunkt seinen Zustand ändert.

Berechnete Werte für Versagenswahrscheinlichkeit bei Anforderung (PFD), Versagenswahrscheinlichkeit pro Stunde (PFH) und mittleren Ausfallabstand (MTBF)



Modell	Prüfintervall (Betriebszeit)		PFD (1/Stunde)	PFH (1/Stunde)	MTBF (Stunden)
	Jahr	Stunden			
1734-IB8S	1	8760	5,85E-07	1,34E-10	5,76E+06
	2	17 520	1,17E-06		
	5	43 800	2,93E-06		
	10	87 600	5,86E-06		
	20	175 200	1,17E-05		
1734-OB8S	1	8760	6,05E-07	1,38E-10	4,57E+06
	2	17 520	1,21E-06		
	5	43 800	3,03E-06		
	10	87 600	6,06E-06		
	20	175 200	1,21E-05		

Referenzinformationen zur Konfiguration

Inhalt dieses Anhangs

Dieser Anhang enthält Informationen zu den Konfigurationseinstellungen.

Informationen zu den Parametergruppen

Die Module weisen die folgenden Parametergruppen auf: Parameter für Sicherheitseingänge, Parameter für Testausgänge, Parameter für Sicherheitsausgänge. Informationen zu den Einstellungen in den einzelnen Parametergruppen finden Sie in den Tabellen. Alle Parameter werden mithilfe der Software RSLogix 5000 festgelegt.

Parameter für Sicherheitseingänge[a]

Parametername		Wert	Beschreibung
x	Input Delay Time Off -> On (Eingangsverzögerungszeit von AUS nach EIN)	0–126 ms (in Inkrementen von 6 ms)	Filterzeit für die Transition von AUS nach EIN
x	Input Delay Time On -> Off (Eingangsverzögerungszeit von EIN nach AUS)	0–126 ms (in Inkrementen von 6 ms)	Filterzeit für die Transition von EIN nach AUS
x	Input Point Mode (Eingangspunktmodus)	Not Used (Nicht verwendet)	Externes Eingangsgerät ist nicht angeschlossen.
		Safety Pulse Test (Sicherheitsimpulstest)	Wird mit einem Kontaktausgangsgerät und in Kombination mit einem Testausgang verwendet. Mit dieser Einstellung können Kurzschlüsse zwischen Eingangssignalleitungen und dem Netzteil (positive Seite) sowie Kurzschlüsse zwischen den Eingangssignalleitungen erkannt werden.
		Safety (Sicherheit)	Es ist ein Sicherheitssensor mit Halbleiterausgang angeschlossen.
		Standard	Es ist ein Standardgerät, wie z. B. ein Reset-Schalter, angeschlossen.
x	Safety Input Test Source (Quelle für Sicherheitseingangstest)	Not Used (Nicht verwendet)	Der Testausgang, der mit dem Eingang verwendet wird.
		Test Output 0 (Testausgang 0)	
		Test Output 1 (Testausgang 1)	
		Testausgang 2	
		Test Output 3 (Testausgang 3)	

Parameter für Sicherheitseingänge[a]

Parametername		Wert	Beschreibung	
x	Input Point Operation Type (Art des Eingangspunktbetriebs)	Single Channel (Einzelkanal)	Wird als Einzelkanal verwendet.	
		Dual-channel Equivalent (Zweikanalig gleichwertig)	Wird als Doppelkanal verwendet. Normal, wenn beide Kanäle ein- oder ausgeschaltet sind.	
		Dual-channel Complementary (Zweikanalig komplementär)	Wird als Doppelkanal verwendet. Normal, wenn ein Kanal ein- und der andere ausgeschaltet ist.	
x	Safety Input Error Latch Time (Selbsthaltezeit für Sicherheitseingangsfehler)	0–65 530 ms (in Inkrementen von 10 ms)	Sicherheitseingangs- oder Testausgangsfehler werden für diese Zeit gesperrt.	1000 ms

a. Parameter, die sich direkt auf die Sicherheit beziehen, sind in der linken Spalte mit einem X markiert.

Parameter für Testausgänge[a]

Parametername		Wert	Beschreibung	Standardwert
x	Test Output Mode (Testausgangsmodus)	Not Used (Nicht verwendet)	Es ist kein externes Gerät angeschlossen.	Not Used (Nicht verwendet)
		Standard	Der Ausgang ist an einem Standardgerät angeschlossen.	
		Pulse Test (Impulstest)	Es ist ein Kontaktausgangsgerät angeschlossen. Wird in Kombination mit einem Sicherheitseingang verwendet.	
		Power Supply (Netzteil)	Das Netzteil eines Sicherheitssensors ist angeschlossen. Die an das E/A-Netzteil (V, G) gelieferte Spannung stammt von der Testausgangsklemme.	
		Muting Lamp Output (Ausgang Muting-Leuchte) (nur Klemme T1 oder T3)	Es ist eine Anzeige angeschlossen und eingeschaltet, damit unterbrochene Leitungen in einer externen Anzeige erkannt werden können.	
	Test Output Fault Action (Aktion bei Testausgangsfehler)	Clear OFF (AUS löschen)	Auszuführende Aktion, wenn ein Kommunikationsfehler erkannt wird.	Clear OFF (AUS löschen)
		Hold Last Data (Letzte Daten halten)		

a. Parameter, die sich direkt auf die Sicherheit beziehen, sind in der linken Spalte mit einem X markiert.

Parameter für Sicherheitsausgänge[a]

Parametername		Wert	Beschreibung	Standardwert
x	Output Point Mode (Ausgangspunktmodus)	Not Used (Nicht verwendet)	Es ist kein externes Ausgangsgerät angeschlossen.	Not Used (Nicht verwendet)
		Safety (Sicherheit)	Wenn der Ausgang eingeschaltet ist, wird der Testimpuls nicht ausgegeben (bleibt eingeschaltet).	
		Safety Pulse Test (Sicherheitsimpulstest)	Mit dieser Funktion können Kurzschlüsse zwischen Ausgangssignalleitungen und dem Netzteil (positive Seite) sowie Kurzschlüsse zwischen den Ausgangssignalleitungen selbst erkannt werden.	

Parameter für Sicherheitsausgänge[a]

x	Output Point Operation Type (Art des Ausgangspunktbetriebs)	Single Channel (Einzelkanal)	Wird als Einzelkanal verwendet.	Dual-channel (Zweikanalig)
		Dual-channel (Zweikanalig)	Wird als Doppelkanal verwendet. Wenn beide Kanäle den Normalzustand aufweisen, können die Ausgänge eingeschaltet werden.	
x	Safety Output Error Latch Time (Selbsthaltezeit für Sicherheitsausgangsfehler)	0–65 530 ms (in Inkrementen von 10 ms)	Sicherheitsausgangsfehler werden für diese Zeit gesperrt.	1000 ms

a. Parameter, die sich direkt auf die Sicherheit beziehen, sind in der linken Spalte mit einem X markiert.

Sonstige Parameter

Parametername	Wert	Beschreibung	Standardwert
Test Output Idle State (Leerlaufzustand des Testausgangs)[a]	Clear OFF (AUS löschen) oder Keep Output Data (Letzte Daten halten)	Definition der Ausgangsdaten befindet sich im Leerlaufzustand.	Clear OFF (AUS löschen)

a. **Nur** über die explizite Nachrichtenübertragung festlegen. Weitere Informationen hierzu finden Sie in Anhang A.

Spezifikationen

Einleitung

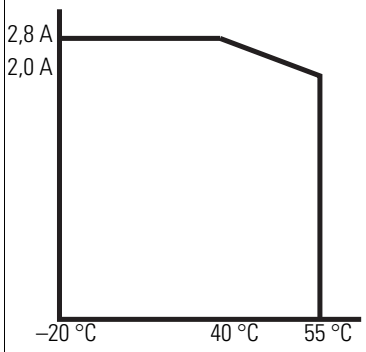
Lesen Sie bei Bedarf die Spezifikationen zu den folgenden Modulen.

Thema	Seite
1734-OB8S – Technische Daten	157
1734-IB8S und 1734-OB8S – Physische Spezifikationen	158
1734-IB8S und 1734-OB8S – Umgebungsspezifikationen	159
1734-IB8S und 1734-OB8S – Zertifizierungen	160

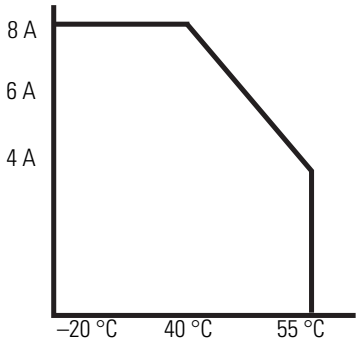
1734-IB8S – Technische Daten

Attribut	Wert
Sicherheitseingang	
Eingänge je Modul	8
Eingangstyp	Stromziehend
Spannung, Eingang im EIN-Zustand	11–30 V Gleichstrom
Max. Spannung, Eingang im AUS-Zustand	5 V Gleichstrom
Min. Strom, Eingang im EIN-Zustand	3,3 mA
Max. Strom, AUS-Zustand	1,3 mA
IEC 61131-2 (Eingangstyp)	Typ 3
Reaktionszeit	<16,2 ms

1734-IB8S – Technische Daten

Attribut	Wert
Impulstestausgang	
Ausgangstyp	Stromspeisend
Anzahl der Quellen (T0, T1M, T2, T3M)	4
Testausgangsstrom (je Ausgangspunkt)	0,7 A max.
Summenstrom der Testausgänge je Modul	2,8 A bei 40 °C
1734-IB8S-Temperatur im Vergleich zur Stromminderung für horizontale und vertikale Installationen	
Max. Restspannung	1,2 V
Max. Ausgangsleckstrom	0,1 mA
Kurzschlussschutz	Ja
Max. Strom (bei Verwendung zum Steuern der Muting-Leuchte)	25 mA Strom, max. (zur Vermeidung eines Fehlers bei Verwendung als Ausgang für die Muting-Leuchte)
Min. Strom (bei Verwendung zum Steuern der Muting-Leuchte)	5 mA Strom, min. (bei dem eine Fehleranzeige generiert wird, wenn als Ausgang für die Muting-Leuchte verwendet)

1734-OB8S – Technische Daten

Attribut	Wert
Sicherheitsausgang	
Ausgänge je Modul	8
Ausgangstyp	Stromspeisend
Ausgangsstrom (je Ausgangspunkt)	1 A max.
Restspannung (Abfall)	<0,6 V
Max. Leckstrom	0,1 mA
Kurzschlusserkennung	Ja (Erkennung kurzzeitig hoher und niedriger Werte sowie von Querschlussfehlern)
Kurzschlussschutz	Elektronisch
Summenstrom der Ausgänge je Modul	8 A (4 A je Klemmeneinheit) bei 40 °C
1734-OB8S-Temperatur im Vergleich zur Stromminderung für horizontale und vertikale Installationen	
Reaktionszeit	<6,2 ms

1734-IB8S und 1734-OB8S – Technische Daten

Attribut	1734-IB8S	1734-OB8S
POINTBus		
Max. POINTBus-Strom	175 mA	190 mA
Verlustleistung	1,4 W	1,9 W
Wärmeabstrahlung	4,8 BTU/h	6,5 BTU/h
Isolationsspannung	50 V (kontinuierlich), Basistrennungstyp zwischen Feldseite und System Keine Trennung zwischen den einzelnen Kanälen Typprüfung bei 707 V DC für 60 s	
Sammelschiene, Betriebsspeisespannung	24 V DC Nennwert	
Sammelschiene, Betriebsspannungsbereich	19,2–28,8 V Gleichstrom	
Eingangsfilterzeit, AUS nach EIN[a]	0–126 ms (in Inkrementen von 6 ms)	
Eingangsfilterzeit, EIN nach AUS[(a)]		
Schraub-Anzugsmoment für Klemmeneinheit	Siehe Spezifikationen für Klemmeneinheit	
Anzeigen	1 gelbe Verriegelungsstatusanzeige 1 grüne/gelbe Stromstatusanzeige 8 E/A-Kanalstatusanzeigen	

a. Die AUS-nach-EIN-Filterzeit am Eingang bezeichnet die Dauer vom Empfang eines gültigen Eingangssignals bis zu dessen Erkennung durch das Modul. Die EIN-nach-AUS-Zeit am Eingang bezeichnet die Dauer vom Empfang eines gültigen Eingangssignals bis zu dessen Erkennung durch das Modul.

1734-IB8S und 1734-OB8S – Physische Spezifikationen

Attribut	Wert
Schlüsselschalterpositionen (links und rechts)	1734-IB8S: Schlüssel 1 = 8 (links); Schlüssel 2 = 1 (rechts) 1734-OB8S: Schlüssel 1 = 8 (links); Schlüssel 2 = 2 (rechts)
Bemessungswert für Steuerlasten	Nicht benannt (nur 1734-OB8S)
Nordamerikanischer Temperaturcode	T4
IEC-Temperaturcode	T4
Gehäusetyp-Nennleistung	Keine (offen)
Verdrahtungskategorie[a]	2 – an den Signalanschlüssen
Drahtgröße	Wird durch installierte Klemmenleiste bestimmt
Gewicht, ca.	62,4 g
Abmessungen (H x B x T), ca. (ohne Klemmenleiste)	77 x 25 x 55 mm

a. Verwenden Sie diese Informationen zur Leiterkategorie zum Planen der Leiterführung. Siehe auch die Publikation 1770-4.1, Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen.

1734-IB8S und 1734-OB8S – Umgebungsspezifikationen

Attribut	Wert
Temperatur, Betrieb	IEC 60068-2-1 (Test Ad, Betrieb bei Kälte), IEC 60068-2-2 (Test Bd, Betrieb bei trockener Hitze), IEC 60068-2-14 (Test Nb, Betrieb bei Temperaturschock): –20 bis 55 °C
Temperatur, Ruhezustand	IEC 60068-2-1 (Test Ab, unverpackt, Ruhezustand, Kälte), IEC 60068-2-2 (Test Bb, unverpackt, Ruhezustand, trockene Hitze), IEC 60068-2-14 (Test Na, unverpackt, Ruhezustand, Temperaturschock): –40 bis 85 °C
Relative Luftfeuchtigkeit	IEC 60068-2-30 (Test Db, unverpackt, feuchte Hitze): 5–95 %, nicht kondensierend
Vibration	IEC 60068-2-6, (Test Fc, Betrieb) 5 g bei 10–500 Hz
Stoßeinwirkung, Betrieb	IEC 60068-2-27 (Test Ea, unverpackt, Stoßeinwirkung) 30 g
Stoßeinwirkung, Ruhezustand	IEC 60068-2-27 (Test Ea, unverpackt, Stoßeinwirkung) 50 g
Emissionen	CISPR 11: Gruppe 1, Klasse A
Störfestigkeit	IEC 61000-4-2: 6 kV Kontaktentladungen 8 kV Luftentladungen
Störfestigkeit bei abgestrahlten Hochfrequenzstörungen	IEC 61000-4-3: 10 V/m mit 1 kHz Sinuswelle 80 % von 80 bis 2000 MHz 10 V/m mit 200 Hz 50 % Impuls 100 % AM bei 900 MHz 10 V/m mit 200 Hz 50 % Impuls 100 % AM bei 1890 MHz 3 V/m mit 1 kHz Sinuswelle 80 % AM von 2000 bis 2700 MHz
EFT/B-Störfestigkeit	IEC 61000-4-4: ±3 kV bei 5 kHz an den Signalanschlüssen
Überspannungsstörfestigkeit	IEC 61000-4-5: ±1 kV Leiter-Leiter (DM) und ±2 kV Leiter-Erde (CM) an den Signalanschlüssen
Störfestigkeit bei leitungsgeführten Hochfrequenzstörungen	IEC 61000-4-6: 10 V eff. mit 1 kHz Sinuswelle 80 % AM von 150 kHz bis 80 MHz

1734-IB8S und 1734-OB8S – Zertifizierungen

Zertifizierung	Wert	
Zertifizierungen: (sofern das Produkt entsprechend gekennzeichnet ist)[a]	**c-UL-us**	Aufgelistet in Industrial Control Equipment, zertifiziert für USA und Kanada. Siehe UL-File E65584. UL-Auflistung für Klasse I, Division 2 Gruppen A, B, C, D Explosionsgefährdete Standorte, zertifiziert für USA und Kanada. Siehe UL-File E194810.
	CE	Europäische Union 2004/108/EG EMV-Richtlinie, konform mit: EN 61326-1; Elektrische Mess-, Steuer-, Regel- und Laborgeräte, Industrielle Anforderungen EN 61000-6-2; Störfestigkeit für Industriebereich EN 61000-6-4; Störaussendung für Industriebereich EN 61131-2; Speicherprogrammierbare Steuerungen (Klausel 8, Zone A & B)
	Ex	Europäische Union 94/9/EG ATEX Richtlinie, konform mit: EN 60079-15; Elektrische Betriebsmittel für gasexplosionsgefährdete Bereiche, Zündschutzart „n" EN 60079-0; Allgemeine Anforderungen II 3 G Ex nA IIC T4X
	C-Tick	Australian Radiocommunications Act konform mit AS/NZS CISPR 11, Industrial Emissions
	TÜV	TÜV-zertifiziert für funktionale Sicherheit[b] bis SIL 3 (IEC 61508, IEC 62061) und PL e/Kategorie 4 (ISO 13849-1)
	ODVA	ODVA-Konformität getestet gemäß den Spezifikationen für CIP Safety im DeviceNet-Netzwerk

a. Konformitätserklärung, Zertifikate und weitere Details zur Zertifizierung erhalten Sie über den Link „Product Certification" (Produktzertifizierung) unter http://www.ab.com.

b. Bei Verwendung mit bestimmten Firmwareversionen.

E/A-Baugruppen

Einleitung

Die folgenden Tabellen enthalten Informationen zu Eingangs-, Ausgangs- und Konfigurationsbaugruppen.

Thema	Seite
Eingangsbaugruppen	161
Ausgangsbaugruppen	163
Konfigurationsbaugruppen	164

Eingangsbaugruppen

Instanz Hex (dezimal)	Modul	Verbindungstyp	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
204	1734-IB8S	Sicherheit und Standard	0	Sicherheitseingang 7	Sicherheitseingang 6	Sicherheitseingang 5	Sicherheitseingang 4	Sicherheitseingang 3	Sicherheitseingang 2	Sicherheitseingang 1	Sicherheitseingang 0
224	1734-IB8S	Sicherheit und Standard	0	Sicherheitseingang 7	Sicherheitseingang 6	Sicherheitseingang 5	Sicherheitseingang 4	Sicherheitseingang 3	Sicherheitseingang 2	Sicherheitseingang 1	Sicherheitseingang 0
			1	Status Sicherheitseingang 7	Status Sicherheitseingang 6	Status Sicherheitseingang 5	Status Sicherheitseingang 4	Status Sicherheitseingang 3	Status Sicherheitseingang 2	Status Sicherheitseingang 1	Status Sicherheitseingang 0
300	1734-IB8S	Nur Standard	0	Reserviert							Fehler Eingangsleistung
314	1734-IB8S	Sicherheit und Standard	0	Sicherheitseingang 7	Sicherheitseingang 6	Sicherheitseingang 5	Sicherheitseingang 4	Sicherheitseingang 3	Sicherheitseingang 2	Sicherheitseingang 1	Sicherheitseingang 0
			1	Kombinierter Sicherheitseingangsstatus	Reserviert	Fehler Eingangsleistung[a]	Reserviert	Reserviert	Reserviert	Status Muting-Leuchte 3	Status Muting-Leuchte 1

Instanz Hex (dezimal)	Modul	Verbindungstyp	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
334	1734-IB8S	Sicherheit und Standard	0	Sicherheitseingang 7	Sicherheitseingang 6	Sicherheitseingang 5	Sicherheitseingang 4	Sicherheitseingang 3	Sicherheitseingang 2	Sicherheitseingang 1	Sicherheitseingang 0
			1	Status Sicherheitseingang 7	Status Sicherheitseingang 6	Status Sicherheitseingang 5	Status Sicherheitseingang 4	Status Sicherheitseingang 3	Status Sicherheitseingang 2	Status Sicherheitseingang 1	Status Sicherheitseingang 0
			2	Reserviert		Fehler Eingangsleistung[a]	Reserviert			Status Muting-Leuchte 3	Status Muting-Leuchte 1
364	1734-IB8S	Sicherheit und Standard	0	Sicherheitseingang 7	Sicherheitseingang 6	Sicherheitseingang 5	Sicherheitseingang 4	Sicherheitseingang 3	Sicherheitseingang 2	Sicherheitseingang 1	Sicherheitseingang 0
			1	Status Sicherheitseingang 7	Status Sicherheitseingang 6	Status Sicherheitseingang 5	Status Sicherheitseingang 4	Status Sicherheitseingang 3	Status Sicherheitseingang 2	Status Sicherheitseingang 1	Status Sicherheitseingang 0
			2	Reserviert				Status Testausgang 3	Status Testausgang 2	Status Testausgang 1	Status Testausgang 0
			3	Reserviert		Fehler Eingangsleistung[a]	Reserviert			Status Muting-Leuchte 3	Status Muting-Leuchte 1
383	1734-IB8S	Standard	0	Reserviert							Fehler Eingangsleistung
			1	Reserviert				Status Testausgang 3	Status Testausgang 2	Status Testausgang 1	Status Testausgang 0
244	1734-OB8S	Sicherheit und Standard	0	Status Sicherheitsausgang 7	Status Sicherheitsausgang 6	Status Sicherheitsausgang 5	Status Sicherheitsausgang 4	Status Sicherheitsausgang 3	Status Sicherheitsausgang 2	Status Sicherheitsausgang 1	Status Sicherheitsausgang 0
404	1734-OB8S	Sicherheit und Standard	0	Status Sicherheitsausgang 7	Status Sicherheitsausgang 6	Status Sicherheitsausgang 5	Status Sicherheitsausgang 4	Status Sicherheitsausgang 3	Status Sicherheitsausgang 2	Status Sicherheitsausgang 1	Status Sicherheitsausgang 0
			1	Überwachung Sicherheitsausgang 7	Überwachung Sicherheitsausgang 6	Überwachung Sicherheitsausgang 5	Überwachung Sicherheitsausgang 4	Überwachung Sicherheitsausgang 3	Überwachung Sicherheitsausgang 2	Überwachung Sicherheitsausgang 1	Überwachung Sicherheitsausgang 0

Instanz Hex (dezimal)	Modul	Verbindungstyp	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
414	1734-OB8S	Sicherheit und Standard	0	Überwachung Sicherheitsausgang 7	Überwachung Sicherheitsausgang 6	Überwachung Sicherheitsausgang 5	Überwachung Sicherheitsausgang 4	Überwachung Sicherheitsausgang 3	Überwachung Sicherheitsausgang 2	Überwachung Sicherheitsausgang 1	Überwachung Sicherheitsausgang 0
			1	Reserviert	Kombinierter Ausgangsstatus	Reserviert	Fehler Ausgangsleistung	Reserviert			

a. Bei diesen Daten handelt es sich ausschließlich um Diagnosedaten. Es liegt **keine** Sicherheitsintegrität vor.

Ausgangsbaugruppen

Instanz Hex (dezimal)	Modul	Verbindungstyp	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
21	1734-IB8S	Sicherheit[a]	0	Reserviert				Standardausgang 3	Standardausgang 2	Standardausgang 1	Standardausgang 0
234	1734-OB8S	Nur Sicherheit	0	Sicherheitsausgang 7	Sicherheitsausgang 6	Sicherheitsausgang 5	Sicherheitsausgang 4	Sicherheitsausgang 3	Sicherheitsausgang 2	Sicherheitsausgang 1	Sicherheitsausgang 0

a. Nur die Ausgänge 1 und 3 können als Muting- oder Testausgänge konfiguriert werden. Auf diese Baugruppe kann nur über eine Sicherheitsverbindung zugegriffen werden.

Konfigurationsbaugruppen

Die Daten für die 1734-IB8S- oder 1734-OB8S-Konfigurationsbaugruppen entnehmen Sie bitte der entsprechenden Tabelle.

1734-OB8S-Konfigurationsbaugruppe

Instanz Hex (dezimal)	Modul	Byte	Feld	Klasse (Hex)	Instanz (dezimal)	Attribut (dezimal)
360	1734-OB8S	0	Safety Output Error Latch Time (Selbsthaltezeit für Sicherheitsausgangsfehler) (niederwertiges Byte)	3B	0	8
		1	Safety Output Error Latch Time (Selbsthaltezeit für Sicherheitsausgangsfehler) (höherwertiges Byte)			
		2	Safety Output 0 Channel Mode (Kanalmodus Sicherheitsausgang 0)	3B	1	6
		3	Safety Output 1 Channel Mode (Kanalmodus Sicherheitsausgang 1)		2	
		4	Safety Output 2 Channel Mode (Kanalmodus Sicherheitsausgang 2)		3	
		5	Safety Output 3 Channel Mode (Kanalmodus Sicherheitsausgang 3)		4	
		6	Safety Output 4 Channel Mode (Kanalmodus Sicherheitsausgang 4)		5	
		7	Safety Output 5 Channel Mode (Kanalmodus Sicherheitsausgang 5)		6	
		8	Safety Output 6 Channel Mode (Kanalmodus Sicherheitsausgang 6)		7	
		9	Safety Output 7 Channel Mode (Kanalmodus Sicherheitsausgang 7)		8	
		10	Dual-channel Safety Output 0 Mode (Modus zweikanaliger Sicherheitsausgang 0)	3F	1	3
		11	Dual-channel Safety Output 1 Mode (Modus zweikanaliger Sicherheitsausgang 1)		2	
		12	Dual-channel Safety Output 2 Mode (Modus zweikanaliger Sicherheitsausgang 2)		3	
		13	Dual-channel Safety Output 3 Mode (Modus zweikanaliger Sicherheitsausgang 3)		4	

1734-IB8S-Konfigurationsbaugruppe

Instanz Hex (dezimal)	Modul	Byte	Feld	Klasse (Hex)	Instanz (dezimal)	Attribut (dezimal)
360	1734-IB8S	0	Test Output 0 Mode (Modus Testausgang 0)	9	1	13
		1	Test Output 1 Mode (Modus Testausgang 1)		2	
		2	Test Output 2 Mode (Modus Testausgang 2)		3	
		3	Test Output 3 Mode (Modus Testausgang 3)		4	
		4	Safety Input Error Latch Time (Selbsthaltezeit für Sicherheitseingangsfehler) (niederwertiges Byte)	3D	0	8
		5	Safety Input Error Latch Time (Selbsthaltezeit für Sicherheitseingangsfehler) (höherwertiges Byte)			
		6	Safety Input 0 Off_On_Delay (Aus_Ein_Verzögerung für Sicherheitseingang 0) (niederwertiges Byte)		1	5
		7	Safety Input 1 Off_On_Delay (Aus_Ein_Verzögerung für Sicherheitseingang 1) (höherwertiges Byte)			
		8	Safety Input 0 On_Off_Delay (Ein_Aus_Verzögerung für Sicherheitseingang 0) (niederwertiges Byte)			6
		9	Safety Input 0 On_Off_Delay (Ein_Aus_Verzögerung für Sicherheitseingang 0) (höherwertiges Byte)			
		10	Safety Input 0 Channel Mode (Kanalmodus Sicherheitseingang 0)			8
		11	Safety Input 0 Test Source (Testquelle Sicherheitseingang 0)			9
		…	Konfigurationsdaten für Sicherheitseingang 1–6		…	…
		48	Safety Input 7 Off_On_Delay (Aus_Ein_Verzögerung für Sicherheitseingang 7) (niederwertiges Byte)		8	5
		49	Safety Input 7 Off_On_Delay (Aus_Ein_Verzögerung für Sicherheitseingang 7) (höherwertiges Byte)			
		50	Safety Input On_Off_Delay (Ein_Aus_Verzögerung für Sicherheitseingang) (niederwertiges Byte)			6
		51	Safety Input On_Off_Delay (Ein_Aus_Verzögerung für Sicherheitseingang) (höherwertiges Byte)			
		52	Safety Input 7 Channel Mode (Kanalmodus Sicherheitseingang 7)			8
		53	Safety Input 7 Test Source (Testquelle Sicherheitseingang 7)			9
		54	Dual-channel Safety Input 0 Mode (Modus zweikanaliger Sicherheitseingang 0)	348	1	3
		55	Pad Byte (Füllbyte) (0x00)	…	…	…
		56	Dual-channel Safety Input 0 Discrepancy Time (Diskrepanzzeit zweikanaliger Sicherheitseingang 0) (niederwertiges Byte)	348	1	5
		57	Dual-channel Safety Input 0 Discrepancy Time (Diskrepanzzeit zweikanaliger Sicherheitseingang 0) (höherwertiges Byte)			
		…	Dual-channel Safety Input 1…2 Configuration (Konfiguration des zweikanaligen Sicherheitseingangs 1–2)	…	…	…
		66	Dual-channel Safety Input 3 Mode (Modus zweikanaliger Sicherheitseingang 3)	348	4	3
		67	Pad Byte (Füllbyte) (0x00)	…	…	…
		68	Dual-channel Safety Input 3 Discrepancy Time (Diskrepanzzeit zweikanaliger Sicherheitseingang 3) (niederwertiges Byte)	348	4	5
		69	Dual-channel Safety Input 3 Discrepancy Time (Diskrepanzzeit zweikanaliger Sicherheitseingang 3) (höherwertiges Byte)			

Weitere Informationen

Zugehörige Dokumentation

Falls Sie zusätzliche Unterstützung beim Einrichten und Verwenden Ihrer Module benötigen, lesen Sie die folgenden Informationen. Technische Daten finden Sie in den entsprechenden Installationsanleitungen. Publikationen stehen unter http://literature.rockwellautomation.com zum Herunterladen bereit. Wenn Sie die gedruckten Versionen technischer Dokumentationen bestellen möchten, wenden Sie sich an Ihren Rockwell Automation-Distributor oder Vertriebspartner.

Quelle	Beschreibung
POINT I/O Selection Guide, Publikation 1734-SG001	Enthält Auswahlinformationen für POINT I/O-Module. Zusätzliche Publikationsreferenzen werden ebenfalls aufgelistet.
Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch, Publikation 1756-RM093	Enthält Referenzinformationen zur Sicherheit und eine Beschreibung des GuardLogix-Steuerungssystems.
GuardLogix-Steuerungen – Benutzerhandbuch, Publikation 1756-UM020	Enthält allgemeine Informationen zur Verwendung von GuardLogix-Steuerungen.
Befehlssatz für GuardLogix-Sicherheitsanwendungen – Referenzhandbuch, Publikation 1756-RM095	Enthält Referenzinformationen, die den Befehlssatz für GuardLogix-Sicherheitsanwendungen beschreiben.
ODVA Media Planning and Installation Guide, http://www.odva.org	Beschreibt die erforderlichen Medienkomponenten sowie deren Einplanung und Installation.
DeviceNet Modules in Logix5000 Control Systems User Manual, Publikation DNET-UM004	Enthält Informationen zum Anschließen der Steuerung an das Netzwerk.
GuardPLC Controller Systems User Manual, Publikation 1753-UM001	Enthält eine Kurzbeschreibung des Sicherheitskonzepts der GuardPLC-Steuerungsfamilie.
GuardPLC Safety Reference Manual, Publikation 1753-RM002	Erläutert, wie das GuardPLC-Steuerungssystem in Sicherheitsanwendungen verwendet werden kann.
Steuerung SmartGuard 600 – Installationsanleitung, Publikation 1752-IN001	Enthält Informationen zur Installation von SmartGuard 600-Steuerungen.
SmartGuard 600-Steuerungen – Sicherheitsreferenzhandbuch, Publikation 1752-RM001	Beschreibt SmartGuard 600-spezifische Sicherheitsanforderungen und Steuerungsmerkmale.
Steuerung SmartGuard 600 – Benutzerhandbuch, Publikation 1752-UM001	Enthält Informationen zum Konfigurieren, Bedienen und Entstören der Steuerung.

Notizen:

Numerics

1734-AENT 19, 78
1734-AENTR 19
1734-EP24DC 67, 68
1734-EPAC 67, 68
1734-FPD 67, 68
1734-IB8S-Feldanschlüsse 51
1734-OB8S-Feldanschlüsse 51
1734-PDN 19
1734-TB 13
1734-TBS 13
1734-TOP 13
1734-TOP3 13
1734-TOP3S 13
1734-TOPS 13

A

abnehmbare Klemmenleiste 13, 49
    anschließen 49
Adapter 19, 78
    EtherNet/IP 13
allgemeine Begriffe 9
Anforderungen für Steuergeräte 35
angefordertes Paketintervall 95
Anschließen
    abnehmbare Klemmenleiste 49
    Modul am Montagesockel 48
ANSI
    B11.19 39
    RIA15.06 39
Anzeige für den Netzwerkstatus 142
Architekturen
    Sicherheit 20
Aus
    Verzögerung 18, 31
    Verzögerungsfunktion 31
    Zustand 15, 31
Ausbauen eines Montagesockels 50
Ausgang
    Baugruppen 163
    Daten 93
    Konfigurationsdialogfeld 103
    Konfigurationsregisterkarte 103
    Leistungsfehler-Bit 93
    Punkt 114
    Rücklesung 93
    Sicherheitszustand 15
    Signale 18
    Verbindung 116
Austausch
    Module 36, 123, 126, 130
Azeton 17

B

Beispiel für vertauschte Kabel 124
Benzol 17
Bewährungsprüfung 10
blockierende höherwertige Fehler 34

C

Chassiserdung 46
CIP Safety 123
    Protokoll 17, 140
Codierung deaktivieren 77, 80

D

Datenpaketgröße 119
DeviceNet-Sicherheit
    Architektur 20
    Konformitätstest 36
Dialogfeld
    „Input Configuration“ (Eingangskonfiguration) 98
    Ausgangskonfiguration 103
    Sicherheit 94
    Testausgangskonfiguration 102
diese Steuerung 84, 91
DIN-Schiene 46
Diskrepanzzeit 18, 27, 98
Draht
    Beispiele 61
    Leiter 16
    Module 50
    Vorsichtsmaßnahmen 17
Drahtbrucherkennung 18
Drehmomentwerte 17
Drucktaste 59

E

E/A
    Baugruppen 161
    Ersatz 130, 137
    Fehler 18
    Statusdaten 18, 34
E/A-Steuerungsdaten 27

Ein
Verzögerung 18, 31
Verzögerungsfunktion 31
Eingang
Baugruppen 161
Daten 93
Fehlerselbsthaltezeit 101
Konfigurationsregisterkarte 98
Leistungsfehler-Bit 93
Reaktionszeit 32
Signalleitungen 25
Verbindung 116
Verzögerungen 31
Verzögerungszeit 100
einkanalig 23
Sicherheitsschütz 62
Einsatzeignung 14
Einzelkanal
Modus 18, 26
elektronisches Datenblatt 9, 108
elektrostatische Entladung 45
EMV-Richtlinien 38
EN
60204-1 37
62061 37
Endschalter 35
Entladung, elektrostatisch 45
EtherNet/IP
Adapter 13
Sicherheitsarchitektur 20
Etikett 43
EU-Richtlinien 17, 38
Europäische Industrienormen 37
exakte Übereinstimmung 77, 80, 84, 90
externe Mittel 84, 91

F

Fehlererkennung 26, 28, 30, 33
Feld
Anschluss 51
Spannungsversorgung 67
Firmware 14
funktional
Validierungstest 21
Verifizierungstest 21

G

Gate-Überwachungsschalter 61
Geräte, Sicherheit 17
Gesetzgebung und Industrienormen 36
Gleichstromspannung 16
gleichwertig 27, 28
Glossar 9
GuardLogix
Steuerungen im Vergleich zu SmartGuard-Steuerungen 126
System 13
Guardmaster-Produkt 35
GuardShield-Impulstest 113

H

Halbleiterausgänge 18
Handbuchkonventionen 9
Herunterladen der Konfiguration 105, 121

I

ID-Nummer 21
IEC
60204-1 36
61000-6-2 36
61000-6-4 36
61131-2 36, 37
61508 36, 37
62061 36, 37
Impuls
Dauer 24, 32
Test 18
Testausgang, Spezifikationen 156
Zeitraum 24, 32
individuell
Ausgangspunktstatus 34
Ausgangsüberwachung 34
Eingangspunktstatus 34
Sicherheitsausgangsstatus 93
Sicherheitseingangsstatus 93
Testausgangsstatus 34, 93
installieren
abnehmbare Klemmenleiste 49
E/A-Module 48
Montagesockel 46
ISO
13849-1 36, 37

J

Japan 41

K

Kennwort 18
Klemmeneingangsstatus 27

kombiniert
Ausgangsstatus 34
Eingangsstatus 34
Sicherheitsausgangsstatus 93
Sicherheitseingangsstatus 93
Status 118
Kommunikationsfehler 148
kompatibles Modul 77, 80, 84, 90
komplementär 27, 29
Konfiguration
Anzeige für den gesperrten Status 143
Baugruppen 164
Einstellungen 151
herunterladen 105, 121
Referenzinformationen 151
Sicherheit 110
Signatur 97
speichern 105, 121
Verwaltungsrechte 97
Konfigurieren
immer 137
Nur wenn keine Sicherheitssignatur vorhanden ist 130
konfigurieren
Modul 123
Konventionen 9
Kurzschluss
Erkennung 18
zwischen Eingangssignalleitungen 25

L

Leistungsstufe „e" 18
Leiter 16
Lichtgitter 60, 113
Listen mit Aufzählungszeichen 9
logische Diskrepanz 18

M

Master 9
Mean Time Between Failure/Mittlerer Ausfallabstand 9, 149
Modul
Richtlinien 14
Statusanzeige 142
Verriegelungsmechanismus 43
Vorsichtsmaßnahmen 15
Montagesockel
Anschließen des Moduls 48
ausbauen 50
Baugruppe 13
Installation 46
MTBF 9
Siehe „Mittlerer Ausfallabstand".
Muting 118
Leuchte 18
Leuchten-Status 93

N

Nachrichtenbefehle 145
Konfigurieren 146
NFPA 79 39
Normen 37
Gesetzgebung 36
Not-Halt
Schalter 35, 95
Taste 60, 61
zweikanalige Geräte 61
nummerierte Listen 9
Nur Hören 80

O

ODVA 9, 36

P

Parametergruppen 151
PELV 46
PFD 9
Siehe „Versagenswahrscheinlichkeit bei Anforderung".
PFH 9
Siehe „Versagenswahrscheinlichkeit pro Stunde".
physische Spezifikationen 158
PL a, b, c, d, e 37
POINT I/O-Plattform 13, 19
POINTBus
Backplane 67, 68
Spezifikationen 158
Produktspezifikationen 9
Publikation, weiterführende 167
Punktstatus 118

R

Rack-Optimierung 80
redundante Steuerung 18
Reinigen der Module 17
Relais mit zwangsgeführten Kontakten 35

Risikobewertung 14
RPI 95
RSLinx-Software 108
RSLogix-Softwareversion 13
RSWho 108

S

Schalter
Gate-Überwachung 61
Grenzwert 35
Not-Halt 95
Türüberwachung 60
Türverriegelung 35
Schematische Darstellungen 59
Schritte 9
Schütze 35
Schutz-Kleinspannung 46
SELV 46
Serie 100S 35
Serie 440G 35
Serie 440H 35
Serie 440K 35
Serie 440P 35
Serie 700S 35
Serie 800F 35
Serie 800T 35
Serie 802T 35
Sicherheit 18
Administrator 14, 16
Anwendungsanforderungen 21
Anzeige für Ausgangsstatus 144
Anzeige für den Eingangsstatus 143
Ausgang mit Testimpuls 32
Ausgänge 16, 18, 23, 32, 33, 34, 118
Ausgangsdaten 93
Ausgangsmodule 88
Ausgangsspezifikationen 157
Ausgangsstatus 148
Eingänge 17, 18, 24, 34, 118
Eingangsdaten 26, 31, 93
Eingangsmodule 82
Eingangsstatus 26, 147
Geräte 17
Kleinspannung 46
Konfiguration 110
Nachrichten 19
Netzwerknummer 21, 123, 125
Registerkarte 94
Sensoren 35
Signatur 21
Steuerung 21
Systemarchitektur 19
Überwachung 118
Vorsichtsmaßnahmen 36
Wiederherstellung nach einem Ausgangsfehler 33
Wiederherstellung nach einem Eingangsfehler 31
Zustand 15, 23
Sicherheits-
netzwerknummer 10
Sicherheitsintegritätsstufe 3 17, 21
Sicherheitskategorie 2 62
Sicherheitskategorie 3 18, 61
Sicherheitskategorie 4 17, 18, 21, 61, 64
SIL 2 18
SIL 3 17, 21
Slaves 9
SmartGuard
Steuerungen im Vergleich zu GuardLogix-Steuerungen 126
System 13
SNN 10, 21
Siehe Sicherheits-netzwerknummer.
Software RSNetWorx for DeviceNet 107, 108
Spannungsversorgung
Beispiele für Netzteile 68
Feld 67
Status 118
Statusanzeige 143
Speichern der Konfiguration 105, 121
Speicherprogrammierbare Steuerungen 20
Standard 10
Ausgänge 18
Ausgangsdaten 93
Statusanzeigen 141
Konfiguration 143
Modul 142
Netzwerk 142
sicherer Ausgang 144
sicherer Eingang 143
Spannungsversorgung 143
Steuergeräte 35
Systemreaktionszeit 21

T

Tags 93
technische Daten 155

Test
Ausgang 18, 24, 34, 118, 148
Registerkarte 102
Status 118, 148
Impuls 24, 32
in einem Zyklus 32
Testausgänge 16, 18
Tür
Überwachungsschalter 60
Verriegelungsschalter 35

U

Überlegungen, Ersetzen 123
UL-Auflistung 39
Umgebung
Spezifikationen 159
und Gehäuse 44
US-Normen 39

V

Verbindung 9
Ausgang 116
Eingang 116
nicht hergestellt, Beispiel 124
Verdünner 17
Versagenswahrscheinlichkeit
bei Anforderung 9, 149
pro Stunde 9, 149
Versagenswahrscheinlichkeit bei Anforderung 21
Versagenswahrscheinlichkeit pro Stunde 21
Verschmutzungsgrad 2 44
Verwendete Begriffe 9
Vorsichtsmaßnahmen 15, 17, 36, 71

W

Weiterführende Publikationen 167
Werte von Tags 93

Z

Zertifizierungen 160
Gehäuse 16
Zustände von Tags 93
Zweikanal
Modus 18, 27
zweikanalig
Einstellung 33
gleichwertig 23, 28
komplementär 29
Sicherheitsschütze 64

Notizen:

Kundendienst von Rockwell Automation

Rockwell Automation stellt im Internet technische Informationen zur Verfügung, um Sie bei der Verwendung seiner Produkte zu unterstützen. Unter http://support.rockwellautomation.com finden Sie technische Handbücher, eine Wissensdatenbank mit Antworten auf häufig gestellte Fragen, technische Hinweise und Applikationsbeispiele, Beispielcode sowie Links zu Software-Servicepaketen. Außerdem finden Sie dort die Funktion „MySupport“, über die Sie diese Tools individuell an Ihre Anforderungen anpassen können.

Zusätzlichen telefonischen Support für die Installation, Konfiguration und Fehlerbehebung erhalten Sie über unsere TechConnect Support-Programme. Wenn Sie weitere Informationen wünschen, wenden Sie sich an Ihren lokalen Distributor oder Ihren Rockwell Automation-Vertreter, oder gehen Sie auf unsere Internet-Seite http://support.rockwellautomation.com.

Unterstützung bei der Installation

Wenn innerhalb der ersten 24 Stunden nach der Installation ein Problem auftritt, lesen Sie bitte die Informationen in diesem Handbuch. Über eine spezielle Kundendienstnummer erhalten Sie Unterstützung beim Einrichten und Inbetriebnehmen Ihres Produkts.

USA	+1 440 646 3434 Montag bis Freitag, 8.00 Uhr bis 17.00 Uhr EST
Außerhalb der USA	Bitte wenden Sie sich bei Fragen zum technischen Support an den für Sie zuständigen Rockwell Automation-Vertreter.

Rückgabeverfahren bei neuen Produkten

Rockwell Automation testet alle Produkte, um sicherzustellen, dass sie beim Verlassen des Werks voll funktionsfähig sind. Sollte das Produkt nicht ordnungsgemäß funktionieren und zurückgegeben werden müssen, gehen Sie wie folgt vor:

USA	Wenden Sie sich an Ihren Distributor. Teilen Sie ihm die Kundendienst-Bearbeitungsnummer mit, die Sie über die oben genannte Telefonnummer erhalten, damit das Rückgabeverfahren abgewickelt werden kann.
Außerhalb der USA	Bitte wenden Sie sich bei Fragen zum Rückgabeverfahren an den für Sie zuständigen Rockwell Automation-Vertreter.

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brüssel, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Düsselberger Straße 15, D-42781 Haan, Tel.: +49 (0)2104 960 0, Fax: +49 (0)2104 960 121
Schweiz: Buchserstrasse 7, CH-5001 Aarau, Tel.: +41(62) 889 77 77, Fax: +41(62) 889 77 11
Österreich: Kotzinastraße 9, A-4030 Linz, Tel.: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation 1734-UM013B-DE-P – Juni 2009
Ersetzt Publikation 1734-UM013A-DE-P – Februar 2009

Copyright © 2009 Rockwell Automation, Inc. Alle Rechte vorbehalten. Printed in USA.